工科离散数学

牛连强　陈　欣　张胜男　编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

离散数学是研究离散结构及其相互关系的数学学科，是计算机科学与技术及其相关专业的理论基础。本书以数理逻辑为基础，介绍命题逻辑、一阶谓词逻辑、集合论、关系、函数、代数结构和图论。

不同于一般的离散数学书籍，本书内容主要以满足一般工科院校计算机科学与技术、软件工程、信息与计算科学以及其他信息领域相关专业的离散数学课程教学要求为主，不求大求全，尤其是根据工程教育的要求，注重介绍有应用价值的理论，避免理论上的缠绕，内容简介务求通俗明了。同时，还增加了相当数量的工程应用方面的简介以及相关参考文献，使学习者能够快速了解这些理论的实际工程用途。

本书的配套网络课程、电子教案和习题辅导用书将陆续推出，以满足现在立体化教学的要求。本书不仅能很好地满足一般工科院校的离散数学课程教学需要，也特别适合自学。

图书在版编目 (CIP) 数据

工科离散数学 / 牛连强，陈欣，张胜男编著. —北京：电子工业出版社，2017.2

ISBN 978-7-121-30641-9

I. ①工… II. ①牛… ②陈… ③张… III. ①离散数学－高等学校－教材 IV. ①O158

中国版本图书馆 CIP 数据核字(2016)第 305974 号

策划编辑：王羽佳
责任编辑：郝黎明
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×980　1/16　印张：12.75　字数：367.2 千字
版　　次：2017 年 2 月第 1 版
印　　次：2017 年 2 月第 1 次印刷
定　　价：35.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010)88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：(010)88254535，wyj@phei.com.cn。

前　言

离散数学是研究离散量的结构及其相互关系的一门学科，是由逻辑学、集合论、关系理论、图论、抽象代数、布尔代数甚至算法设计、组合分析、离散概率和计算模型等汇集起来的一门综合学科。由于数字电子计算机是一个离散结构，只能处理离散的或离散化了的数量关系和数学模型，这正是离散数学的主要内容，因此，离散数学构成了计算机相关学科的基础学科。为此，《中国计算机科学与技术学科教程 2002》将其界定为计算机科学与技术专业的核心基础课程，美国IEEE&ACM 也确定其为计算机专业的核心课程。

应该说，计算机及其相关专业的绝大部分课程，都是直接以离散数学作为理论基础的，也可以说是离散数学的直接运用，或者说需要依靠离散数学课程中建立的观点、方法和逻辑思维能力去解决具体问题。因此，离散数学课程的教学目的就是要建立逻辑（数学）推理能力、了解重要的离散对象与结构、构建和应用解决离散问题的模型及具备算法思维等。

现在有一些相当成功的离散数学教材，如 Kenneth H. Rosen 的《Discrete mathematics and its applications》、左孝凌的《离散数学》和屈婉玲、耿素云的《离散数学》等。在近 30 年的教学实践中，我们采用这些教材取得过一定的成功，但也存在着诸多问题。概括地说，这些教材大而全，更关注理论与系统的完整性，这与教材的定位甚至国家对精品教材、规划教材、优秀教材等的要求和评价标准不无关联，缺乏对学习对象本身的情况和层次、学时的减少以及工程教学目的的变化等实实在在因素的关注。这些问题在湖南大学的张洪圣等老师编写的同名教材中已经部分提及，我们深有同感。举例说，普通工科高校在我国高校中占大多数，但她们的学生与 985、211 高校存在着很大的差异，以学术研究为目标的教材和教学内容上的趋同不仅达不到“拔高”的目标，反而使学生过早丧失了学习兴趣，形成一系列不良的连锁反应。又如，在仅有 48～64 学时的教学时间里，我们不能期望把类似数论、离散概率、组合设计、形式语言、自动机等内容都灌输给普通院校的学生。

本书的写作目的是为一般的而非拔尖的普通工科高校的计算机、软件工程及其相关专业提供一本通俗、易于理解、易于自学、有一定工程应用背景和实际问题引导的教材。因此，本书不追求体系的完整、内容的全面和对理论的深入探讨，也不关注竞赛、考研等问题。为了达到目标，体现自身的特点，我们注重如下问题并采取了我们认为适当的做法：

- **内容按教学实际取舍**。舍弃中学学过的简单组合计数、前文提到的离散概率、数论、组合设计、形式语言等内容，以及数据结构等课程中涵盖的算法，不使内容过于膨胀，并尽量避免与后续课程重复。
- **次序编排突出逻辑思维**。以逻辑学而不是集合论为出发点，用命题逻辑和谓词逻辑主导解决后续所有问题的思维，以便强化分析、解决问题的逻辑性和能力。
- **对问题平实、透彻讲解**。离散数学也是数学，内容抽象。通过信息相关领域实例、问题引

导、分析、评价、辨析等步骤，将问题讲解透彻，避免读者需要花过长的时间思考或借助参考书才能读懂，甚至利用“理解”标签予以提示并展示应理解的程度。特别地，对大量值得注意或认真分析的关键问题，都通过“辨析”标签给出讨论和警示。

- **概括、突出问题核心**。对解决一类问题的核心内容给予总结、概括和突出，说明此类问题的实质和解决方法的关键，而不是给出一个具体题目的解法。
- **适当引入工程问题**。选取相关领域中有代表性的工程应用实践问题作为示例或习题，消除学生总认为学理论与实际脱节的误解，激发其学习课程和解决实际问题的兴趣。
- **对思考和应用进行引导**。作为教材，对于新的成果、大量的相关问题及其解决方案不可能全部囊括，仅是一斑。对于很多问题，通过“延伸”标签指出其发展方向、实际应用案例、存在的解决方法等，并列出可供参考的论文等素材，以引导学生自己探索。当然，这些内容作为课堂的延伸，以辅助学习和思考为主，研究为辅。因此，列出的论文都不是专门研究理论而是程度较浅的应用型文章、教学论文乃至书籍。
- **洗练定理与习题**。过多罗列已有的结果令人眼花缭乱，还会误导学生机械记忆而不是由基本概念出发进行主动思考、探究和发现结果。同时，尽管多做习题有助于问题的理解，但需要大量的时间和精力，过多习题也容易使人恐惧并产生排斥心理。为此，尽量精简了定理与习题。考虑到本课程中概念（定义）对内容理解和题目求解的极端重要性，故将重要概念纳入习题，直接提醒学生弄懂并记住这些定义。

使本书体现上述特点源自于学生的实际情况、教学上的要求以及人才培养工程化的形势变化等因素。我们认为，在把更多的时间、思考、总结、发现任务交给学生时，教师要能使学生学会学习，教材要有助于学生自主学习。教材既不能包罗万象，求深求全，也不能只是“干巴巴”的纲，更不应连一节中有几个重要概念、主要方法之类的总结都由教材代替。考虑到目前离散数学课程多在一年级中开设，我们没有对算法的描述以及程序实现提出过多要求，以免徒增额外负担且冲淡主题。此外，还对重要名词配以英文对照，以期可以辅助对专业外文词汇的掌握。

全书分为 8 章，分别是“命题逻辑”“谓词逻辑”“集合论基础”“关系”“函数”“运算与代数系统”“环、域、格和布尔代数”“图”。这种安排次序的目的是期望以严密的逻辑思维贯穿各部分内容，以使思考和推理更富有理论依据。全书的内容可在 70 个学时内讲完。

本书的几位作者都具有 20 多年的课程教学经验，且未间断地从事本科离散数学课程的教学工作，无论是对课程内容、体系、教学方法和安排，还是工程教育的发展方向与工科学生的实际情况均有着深刻的理解，这使得本书的写作更有针对性。我们期望通过本书使离散数学的内容更容易理解、学习和掌握，促进课程教学质量的提高，但囿于个人见解，仍会存在诸多缺憾，欢迎读者指出其不足，也期待能与读者做更多的交流（niulq@sut.edu.cn）。

此外，本书的出版得到了沈阳工业大学和学校诸多老师的支持和帮助，作者深表感谢！

作　者

目　录

第 1 章　命 题 逻 辑

逻辑（logic）一词源于希腊文 logoc，有“思维”和“表达思考的言辞”之意。逻辑学则是研究思维形式及思维规律的科学。

逻辑分为辩证逻辑和形式逻辑。辩证逻辑是指以辩证法认识论为基础的逻辑学，形式逻辑则是指依据对思维的形式结构和规律进行形式上的推演构成的逻辑学。这里的“形式”是相对于“内涵”（或内容）而言的，形式逻辑只从形式上进行推导，只关心前提和结论之间的逻辑关系而不关心内涵是否真实，故为“形式”上的逻辑。

形式逻辑所研究的思维形式结构就是指概念、判断和推理之间的结构和关系。其中，**概念**是指反映事物本质属性的思维形式，是思维的基本单位。概念用于给一个名词做界定，也是对其公共属性所做的抽象。例如，“商品是用来交换的劳动产品”就描述了一个“商品”的概念。

判断是指对事物是否具有某种属性，即是否符合某概念进行肯定或否定的回答。例如，根据商品的概念，“手机是商品”是一个判断。当然，判断也用于对事物之间是否存在某些关系做回答。

推理是指由一个或几个判断推出另一个判断的思维形式。

现代形式逻辑是利用数学方法或者说借助符号体系进行推理规律研究的，因此，也称为**数理逻辑**或**符号逻辑**，这是《离散数学》课程所讨论的范畴。最早提出用数学方法来描述和处理逻辑问题的学者是德国数学家莱布尼茨（G.W.Leibnitz），经过乔治·布尔（George Boole）、弗雷格（G.Frege）、怀特海（A.N.Whitehead）和罗素（B.Russell）等人的创造性工作，使得数理逻辑形成了专门的学科。1938 年，克劳德·艾尔伍德·香农（Claude Elwood Shannon）在“继电器和开关电路的符号分析”一文中提出利用布尔代数对开关电路进行相关分析，证明了可以通过继电器电路来实现布尔代数的逻辑运算，并给出了实现加、减、乘、除等运算的电子电路设计方法，开启了数理逻辑在开关电路理论和计算机科学方面的应用，也使其成为计算机科学的基础理论之一。

1.1　命　　题

推理是对判断之间的关系进行的逻辑推导，这里的判断称为“命题”。

[定义 1-1] 表达判断的可判别真假的陈述句称为**命题**（proposition 或 statement）。一个命题所表达判断的或“真”或“假”的结果称为命题的**值**或**真值**（truth）。真值为真的命题称为**真命题**，真值为假的命题称为**假命题**。

上述定义说明，命题是一个陈述事实的句子，是应该能够肯定对或错的陈述句，不能非真非假，也不能既真又假。

[辨析] “真值”就是值，只是一种称呼方法，不是“真”的意思。真值可以是真或假。

命题一般用字母来标记，如 p 或 P。例如：p：沈阳是一个大城市。

如果一个命题的真值为真，可用 **T**、1 或“真”表示；若真值为假则用 **F**、0 或“假”表示。可见，p 的值为 1。

[辨析] 用 **T**/**F** 表示逻辑值直观，用 1/0 表示则更接近计算机，也便于演算。这种量在计算机内部或程序设计语言中多用 1/0 表示，称其为逻辑量。

作为代表命题的符号，前述的 p 是**命题常量**（proposition constant），因为它代表一个确定的命题。如果符号 p 可以任意指代，则称为**命题变元**（变量，proposition variable）。不可再拆分的命题称为**原子命题**（atom）或**简单命题**，否则是**复合命题**（compound proposition），即复合命题是由原子命题与联结词构成的命题。

例 1-1 判别下列陈述是否为命题。若是，说明其真值。

(1) 日本人民是伟大的。
(2) 雪是黑的。
(3) $1+101=110$。
(4) 火星上有生物。
(5) 一个偶数可表示成两个素数之和。
(6) $x+y=z$。
(7) 动作快点！
(8) 天安门真雄伟啊！
(9) 请给我一杯茶。
(10) 你掌握命题这个概念了吗？
(11) 我正在说谎。
(12) 我只给不给自己刮胡子的人刮胡子。
(13) 如果天气好，我就去散步。

解 (1) 是命题，值为 1。一个人可能不伟大，但哪国人民都是伟大的，判断命题的真假不能掺杂个人喜好和感情色彩。

(2) 是命题，值为 0。不要管有没有污染，应是客观真相。

(3) 是命题，值因进制不同而不同，给定进制条件后就可确定其值。

(4) 是命题，值目前不能确定，但终究有一天会确定。

(5) 是命题，其值有待证明。此即哥德巴赫猜想。

(6) 不是命题，因为语句中的量都是变量，值不确定。

(7)(8)(9)(10) 不是命题。祈使句、感叹句和疑问句都不是陈述句，自然不是命题。

(11)(12)不是命题。这是一类特殊的句子，称为“悖论”。悖论虽有命题的形式，但不能表示判断，无法确定真假。

[辨析] 悖论近乎诡辩，无法确定真假。若假定其为真，由字面可推出值为假，反之亦然。或者说，悖论不能自圆其说，总存在漏洞。例如，对于(12)，试想：“我”的胡子应由谁来刮？

(13) 是命题。复合命题，其值要依据两个原子命题的值才能确定。

在逻辑学中，命题与判断是两个既有联系又有区别的概念，命题是对事物情况的陈述，判断是对思维对象有所断定的思维形式，是断定者在一定时空条件下对一个命题是真或假的断言。因此，判断一定是命题，而命题不一定是判断。例如，“火星上有生物。”是命题，但没有经过证实，不是判断。

思考与练习 1.1

1-1　何谓形式逻辑？形式逻辑、数理逻辑与符号逻辑是什么关系？我们学习的是什么逻辑？

1-2　何谓命题？何谓命题的真值？如何表示命题的值？何谓复合命题？

1-3　何谓判断？何谓推理？

1-4　下述语句是否为命题？若是，是何种命题，命题的真值是什么？

(1) 下水救人的男孩真勇敢啊！

(2) 下水救人的男孩真勇敢。

(3) $3x+2>0$。

(4) 2 是素数或合数。

(5) 你下午有时间吗？如果有，请到我这儿来一下。

(6) 如果 a 与 b 是对顶角，则角 a 等于角 b。

(7) 做你的作业。

(8) 本语句为假。

1-5　找出命题中的所有原子命题并用符号表示它们。

(1) 李雨春一边看书一边听音乐。

(2) 我不去旅游。

(3) 只有社会主义能够救中国。

(4) 杨明既不在教室，也没在寝室，他出去了。

(5) 当山花开的时候，你爹就回来了。

1.2　逻辑联结词

为了由一个或两个原子命题直接构成复合命题，可以定义 9 个**逻辑联结词**（logical connectives）。自然地，只要联结词使用正确，就可以由原子命题构成新的复合命题。在符号演算时，联结词代表着运算符，命题是参与运算的量。

1.2.1　基本联结词

[定义 1-2] 否定¬。若 p 为命题，新命题¬ p 是对 p 的**否定**（negation，not）。¬ p 的值与 p 相反，读作“非 p”。

这是唯一一个“一元”联结词。C 和 Java 等语言中体现为逻辑否定运算，用!表示。

例 1-2　令 p：沈阳是一个大城市，给出命题¬ p 的描述。

解　¬ p 可以有多种叙述方式，如：

(a) 沈阳不是一个大城市。

(b) 沈阳是一个不大的城市。

(c) 沈阳是一个大城市不真。

[辨析] 从此例可感受到采用符号表示（数学方法）的好处：表示简单且具有唯一性，而用自然语言描述却存在着多种说法，也不严格。

通常，原子命题对应着肯定形式的命题，含有“不”、“非”等联结词的命题则被视为复合命题。例如，用 p 表示原子命题“他是好人”，则命题“他不是好人”构成复合命题 $\neg p$。

[定义 1-3] 合取 $\wedge$（逻辑积）。若 p 和 q 为命题，则 p 和 q 的**合取**（conjunction，and）构成新命题 $p \wedge q$，读作“p 与 q”或“p 与 q 的合取”。当且仅当 p 和 q 都为 1 时，$p \wedge q$ 为 1，否则为 0。

从演算角度看，$p \wedge q$ 表示按逻辑求积，即 $p \wedge q = p \times q$，运算规则为：

$$1\times1=1，\ 1\times0=0，\ 0\times1=0，\ 0\times0=0。$$

自然语言中的联结词“和”、“与”、“且”、“同”、“一边、一边”，以及所有并列句、转折句都对应着合取联结词。在 C 和 Java 等语言中体现为逻辑与运算，用&&表示。

例 1-3 用符号表示命题“不仅 sin$x$ 是奇函数，x^3 也是奇函数”。

解 令 p：sin$x$ 是奇函数，q：x^3 是奇函数，则原命题可表示为：

$$p \wedge q。$$

注意自然语言中的转折句也对应着合取联结词。例如，p：道路曲折，q：前途光明，则命题“道路虽然曲折，但前途光明”应表示为 $p \wedge q$。

[定义 1-4] 析取 $\vee$（逻辑和）。若 p 和 q 为命题，则 p 和 q 的**析取**（disjunction，inclusive or）构成新命题 $p \vee q$，读作“p 或 q”或“p 与 q 的析取”。当且仅当 p 和 q 都为 0 时，$p \vee q$ 为 0，否则为 1。

从演算角度看，$p \vee q$ 表示按逻辑求和，即 $p \vee q = p + q$，运算规则为：

$$1+1=2\ （逻辑意义仍是\ 1），\ 1+0=1，\ 0+1=1，\ 0+0=0。$$

自然语言中的联结词“或”、“或者”和“亦或”均对应于析取联结词。在 C 和 Java 等语言中对应着逻辑或运算，用||表示。

例 1-4 用符号表示命题“马云是阿里巴巴集团主席或首席执行官”。

解 令 p：马云是阿里巴巴集团主席，q：马云是阿里巴巴集团首席执行官，则原命题可表示为：

$$p \vee q。$$

一个非常重要的问题是自然语言中的“逻辑或”包括两类，其一为定义 1-4 中的析取，也称为“可兼析取”，另一类为“不可兼析取”。

[辨析] 析取 $\vee$ 也称“可兼或”或“可兼析取”，这是指 p 和 q 都为 1 时，$p \vee q$ 也为 1，即两者可以兼有。

[定义 1-5] 不可兼析取 $\triangledown$。若 p 和 q 为命题，则 p 和 q 的**不可兼析取**（exclusive or，或称**不可兼或**、**排斥或**）构成新命题 $p \triangledown q$。此命题用于描述两者不能兼有的情况，当且仅当 p 和 q 的真值相同（都为 1 或都为 0）时，$p \triangledown q$ 为 0，否则为 1。

不可兼析取$\triangledown$与著名的“异或”运算（XOR）相对应，也可用$\oplus$表示。对于任意的命题p，有如下运算结果：

$$p \triangledown 0 = p\ ,\quad p \triangledown 1 = \neg p\ ,\quad p \triangledown p = 0\ 。$$

[延伸] 不可兼或的特殊性质使其应用非常广泛。C 和 C++等语言中虽没有对应的逻辑运算，但有按位异或运算^。对于任意的整数a，有

$$a\text{^}0 = a,\quad a\text{^}a = 0。$$

如果屏幕上的一个像素具有颜色b，可以用某种颜色a与其做按位异或^运算，$a\text{^}b$使颜色产生变化。当使用颜色a与其再次运算时，有$a\text{^}(a\text{^}b) = (a\text{^}a)\text{^}b = b$，这就恢复了最初的颜色$b$。这是一种快速“擦除”技术，可用于实现绘图软件中拉伸线条的橡皮筋等功能[1]。

[定义 1-6] 条件$\rightarrow$。若p和q为命题，则p **条件** q（conditional）构成新命题$p \rightarrow q$，读作“p则q”，或“p条件q”，或“如果p那么q”，或“只要p就q”。当且仅当p为 1 而q为 0 时，$p \rightarrow q$为 0，否则为 1。

[辨析] $p \rightarrow q$一般称为条件句，而p和q分别称为“前件”和“后件”。最值得注意的是，当前件p为 0 时，条件句$p \rightarrow q$为 1，与后件q的真假无关。这被称为“善意的推断”。

什么是善意的推断呢？就是前提不成立时命题就真，不用计较结果。考虑如下示例：

“如果我中了彩票，我把一半奖金分给你”。

如果我中了彩票，必须分给你一半奖金才不算食言。但是，当我没中彩票时，无论分给你与否这话都是真的。既然只是“如果”，就是假设。假设不成立，一切休提。

自然语言中的条件联结词很多，包括“因为、所以”、“只要、就”、“仅当”、“当”、“只有、才”、“除非、才”和“除非、否则（非）”等。

例如，令 p：函数$f(x)$在x_0处可导，q：$f(x)$在x_0处连续，则命题“如果函数$f(x)$在x_0处可导，则$f(x)$在x_0处连续”表示为：

$$p \rightarrow q\ 。$$

[定义 1-7] 双条件$\leftrightarrow$。若p和q为命题，则p **双条件** q（biconditional）构成新命题$p \leftrightarrow q$（或$p \rightleftarrows q$）。读作“p双条件q”或“p当且仅当q”。当且仅当p和q的真值相同时，$p \leftrightarrow q$为 1，否则为 0。

很明显，命题$p \leftrightarrow q$表示p和q互为充分必要条件。

例 1-5　用符号表示命题“两个圆S_1和S_2的面积相等的充分必要条件是它们的半径相等”。

解　令p：两个圆S_1和S_2的面积相等，q：它们的半径相等，则原命题可表示为：

$$p \leftrightarrow q\ 。$$

例 1-6　用符号表示命题“你可以坐飞机当且仅当你买了机票”。

解　令p：你可以坐飞机，q：你买了机票，则原命题可表示为：

$$p \leftrightarrow q\ 。$$

在以上 6 个联结词中，$\neg$、$\wedge$、$\vee$是最基本的联结词，其他联结词都可由它们表示出来。例

如，比较 p 和 q 取不同真值时复合命题的真值即可发现，不可兼析取 $\triangledown$ 可以表示为：

$$p \triangledown q = (p \wedge \neg q) \vee (\neg p \wedge q)。$$

观察对联结词 $\triangledown$ 和 $\leftrightarrow$ 的规定还可知：

$$p \triangledown q = \neg(p \leftrightarrow q)。$$

这是两种重要的联结词转换关系。

在自然语言或者说生活中，组成复合命题的原子命题之间是有联系的，组成条件句的两个原子命题一般也会有因果关系，但数理逻辑中并无此要求。例如，下述命题都是正常的：

(1) 程序是用某种语言编制的，而网络是一种重要的交流工具。

(2) 如果天是蓝的，那么，太阳从东方升起。

[延伸] 逻辑联结词的用处广泛，网页中普遍采用逻辑运算进行信息检索，也称作布尔逻辑搜索。此时，联结词（布尔逻辑运算符）的作用是把检索词连接起来，构成一个逻辑检索项。常见的浏览器中可能直接使用 not、and 和 or 表示否定、合取和析取，也可能使用–、&（或空格）和+（或|）等符号表示。例如，Google 中使用–、and 和 or 表示，可用条件表达式“课程 and 教师–学生”表示含有关键词“课程”和“教师”，但不包含“学生”的页面。百度中对应的逻辑联结词为–、空格和|[2]。

1.2.2 其他联结词

[定义 1-8] 与非↑。若 p 和 q 为命题，则 p **与非** q（not and）构成新命题 $p \uparrow q$，含义是 $p \uparrow q = \neg(p \wedge q)$。

[辨析] 与非就是“与的非”，或者说“合取的否定”。

[定义 1-9] 或非↓。若 p 和 q 为命题，则 p **或非** q（not or）构成新命题 $p \downarrow q$，含义是 $p \downarrow q = \neg(p \vee q)$。

[辨析] 或非就是“或的非”，或者说“析取的否定”。

[定义 1-10] 条件否定 $\overset{c}{\rightarrow}$。若 p 和 q 为命题，则 p **条件否定** q（not if then）构成新命题 $p \overset{c}{\rightarrow} q$，含义是 $p \overset{c}{\rightarrow} q \Leftrightarrow \neg(p \rightarrow q)$。条件否定也称为“逆条件”。

通过分析真值的情况容易说明，合取、析取、不可兼析取、与非、或非都满足交换律和结合律。

思考与练习 1.2

1-6 利用开关、电源和一个灯泡描述与否定、合取和析取联结词对应的电路。

1-7 说明 p 和 q 取何值时，命题 $\neg p \rightarrow q$ 为 0？当 p 和 q 的值均为 1 时，命题的真值是什么？

1-8 对于一个命题 p，复合命题 $p \triangledown 1$、$p \triangledown 0$、$p \triangledown p$ 和 $p \triangledown \neg p$ 的真值都是什么？

1-9 对于一个命题 p，复合命题 $p \uparrow p$ 和 $p \downarrow p$ 的真值都是什么？

1-10 写出“–2 是偶数或 3 是正数”的否定命题，再尝试用不同的联结词来表示它。

1-11 “中国和巴基斯坦是兄弟”中的“和”与联结词 $\wedge$ 有何不同？

1-12　写出一个命题，可以表示为符号形式 $p \leftrightarrow (\neg q \wedge r)$。

1-13　令 p：明天下雨，q：我去镇上，那么，$\neg(p \wedge q)$ 和 $p \bar{\vee} q$ 分别表示什么命题？

1-14　用 $\neg$、$\wedge$、$\vee$ 分别表示联结词↑和↓。

1-15　利用百度浏览器搜索含有“XOR”和“异或”这两个词的网页，阅读并尝试找到它们的一些用途。

1.3　命题公式与真值表

1.3.1　命题公式

原子命题或复合命题可以借助联结词再组成复合命题。例如，若 p、q 和 r 均为命题常量，那么，$p \wedge q$ 为复合命题，且 $(p \wedge q) \rightarrow r$ 也是复合命题。当这些命题标识符代表命题变元时，$p \wedge q$ 和 $(p \wedge q) \rightarrow r$ 不再是命题，称其为“命题公式”、“合式公式”或“命题合式公式”，也可简称为“公式”。当然，并不是任意的命题标识符与联结词组成的符号串都是命题公式，需要遵循一定的原则。

[定义 1-11] 命题演算的**合式公式**（well-formed formula，简称 wff）定义为：

(1) 单个命题变元或常量是一个合式公式。

(2) 如果 p 是合式公式，那么 $\neg p$ 是合式公式。

(3) 如果 p 和 q 是合式公式，那么 $p \wedge q$、$p \vee q$、$p \bar{\vee} q$、$p \rightarrow q$ 及 $p \leftrightarrow q$、$p \uparrow q$、$p \downarrow q$、$p \overset{c}{\rightarrow} q$ 都是合式公式。

(4) 当且仅当有限次地应用规则(1)、(2)、(3)所得到的包含命题变元、常量、联结词和括号的符号串是合式公式。

组成合式公式的命题变元（或常量）可称为公式的“分量”。

[理解] 不必深究此定义，它可以被不严格地解释成：由命题常量、变元和联结词组成的有意义的式子就是合式公式。这里的“有意义”就是指要遵循运算规则的要求，如 $(p \wedge 1) \rightarrow q$ 有意义，而 $(\vee p \wedge 1) \neg q$ 则无意义。这与程序设计语言中对表达式的不严格描述是相同的，而命题公式就是命题逻辑中的表达式。

[辨析] 定义中之所以称其为命题公式或合式公式而不是命题，是因为其中可能含有值未知的命题变元，这如同不能说表达式是一个数一样。例如，在 p 和 q 为变元时，命题公式 $(p \wedge 1) \rightarrow q$ 的值是不确定的。

在一个命题公式 A 含有 n 个原子变元时一般可这样描述：

$$A(p_1, p_2, \cdots, p_n) = (p_1 \vee p_2) \rightarrow \cdots。$$

类似地，一个数学表达式一般这样描述：

$$f(x_1, x_2, \cdots, x_n) = (x_1 + x_2) * \cdots。$$

它们没有本质区别，但 x_1，x_2，…，x_n 通常取连续区间的实数，f 亦然。相对地，p_1，p_2，…，

p_n 仅取值为 1 或 0，A 本身亦如此。从这一点上说，命题公式比一般数学表达式更简单。同时，命题公式也称为“命题函数”，公式中的分量就是函数的自变量。

为避免一个命题公式中出现太多括号，规定主要联结词（运算符）的优先次序（优先级）如下：

$$\neg \xrightarrow{\text{优先于}} \wedge \xrightarrow{\text{优先于}} \vee \xrightarrow{\text{优先于}} \rightarrow \xrightarrow{\text{优先于}} \leftrightarrow$$

对于同级运算，$\neg$ 按从右至左的顺序依次进行，其他运算则按从左至右的顺序依次进行。

使用圆括号可以改变或强调运算的优先次序，如 $p \vee q \rightarrow r$ 等同于 $(p \vee q) \rightarrow r$，但不等同于 $p \vee (q \rightarrow r)$。

1.3.2 真值表

为了表示一个联结词的内涵或分析一个命题（公式）的真值情况，可以对命题（公式）中所含有的原子变元的所有可能取值及其对应的命题（公式）的真值进行分析。

[定义 1-12] 若 $p_1, p_2, \cdots, p_n$ 是出现在命题公式 A 中的所有原子变元，任意指定 $p_1, p_2, \cdots, p_n$ 的一组真值称为 A 的一个**解释**（Interpretation），也称为**指派**或**赋值**（assign）。简言之，对一个命题公式的一个解释就是对其所有原子变元的一次赋值。

显然，n 个原子变元共有 2^n 个解释。例如，命题公式 $p \wedge q$ 的 2 个原子变元共有 $2^2=4$ 个解释，分别是 11、10、01 和 00。

[定义 1-13] 将一个命题的所有解释与对应命题的真值汇聚成表称为**真值表**（truth table）。用于规定一个联结词组成的复合命题公式的真值表就是程序设计语言中的运算表。表 1-1 和表 1-2 分别确定了联结词 $\wedge$ 和命题 $\neg p \rightarrow \neg q$ 的真值情况。

表 1-1

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

表 1-2

p	q	$\neg p$	$\neg q$	$\neg p \rightarrow \neg q$
1	1	0	0	1
1	0	0	1	1
0	1	1	0	0
0	0	1	1	1

表 1-3 同时描述了前文定义的 9 个联结词的真值情况。

表 1-3

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$	$p \bar{\vee} q$	$p \uparrow q$	$p \downarrow q$	$p \overset{c}{\rightarrow} q$
1	1	0	1	1	1	1	0	0	0	0
1	0	0	0	1	0	0	1	1	0	1
0	1	1	0	1	1	0	1	1	0	0
0	0	1	0	0	1	1	0	1	1	0

[辨析] 注意真值表中变元赋值的排列顺序。若有 n 个命题变元，按 $2^n-1 \rightarrow 0$ 或 $0 \rightarrow 2^n-1$ 的顺序将这些整数转换为 n 位二进制串排列即可，如 11、10、01、00，这也说明了真值表的行数。

除了表示原子命题的变元外，一个真值表中可以列出一个或几个命题公式的真值，但最后总要包括最关注的命题公式列。

思考与练习 1.3

1-16　何谓命题公式的一个解释？含有 n 个原子变元的公式有多少种解释？

1-17　利用真值表说明联结词 $\wedge$、$\vee$、$\bar{\vee}$、$\uparrow$、$\downarrow$ 均满足结合律和交换律。

1-18　利用真值表说明联结词 $\wedge$ 对 $\vee$ 满足分配律。

1-19　构造下述公式的真值表。

(a) $(p \wedge \neg q) \vee (\neg p \wedge q)$　　(b) $p \rightarrow (q \bar{\vee} r)$

(c) $(\neg p \rightarrow q) \bar{\vee} (p \rightarrow r)$　　(d) $p \rightarrow (q \leftrightarrow s)$

(e) $(p \bar{\vee} q) \downarrow q$

1.4　命 题 翻 译

为了实现符号推导，必须先将自然语言描述的命题用符号表示，称为命题**符号化**或**翻译**。翻译后的符号串应是正确的命题公式。

1.4.1　合取命题

例 1-7　将下述命题用符号表示。

(1) 黄渤既聪明又勤学苦练。　　(2) 黄渤聪明，而且勤学苦练。

(3) 中国人民是勤劳和勇敢的。　　(4) 你是好人，他不是好人。

(5) 他虽然聪明但不用功。　　(6) 我努力了，可是没有达到理想的效果。

(7) 张三或李四都可以做这件事。

解　上述所有复合命题均应表示为两个命题的合取。例如，对于(3)，令 p：中国人民是勤劳的，q：中国人民是勇敢的。则原命题表示为：

$$p \wedge q \text{。}$$

虽然(7)中的命题联结采用了“或”，但重在“都”，是一种不太规范的说法。

[辨析] 注意用符号表示原子命题时不能包括汉语中的联结词，如既、又、而且、虽然、但是等，且需要根据上下文补足句子中省略的成分。

汉语的“和”、“与”等词有特殊的用法，即仅表示原子命题而非合取，如：

(1) 中国和巴基斯坦是全天候战略合作伙伴。

(2) 吾与汝毕力平险。

怎么衡量“p 与 q”、“p 和 q”这样的命题是原子命题还是复合命题呢？通常，如果句子的谓语部分反映的是人或物（如 p 和 q）之间的关系或者共同完成的事情则是原子命题，否则为复合

命题。上述命题(1)中的谓语体现了二者的关系，命题(2)中的谓语描述二者共同做一件事，都是原子命题，而下述命题的谓语则不同：

科比和詹姆斯都是 NBA 明星。

故这是一个由两个原子组成的合取复合命题。

1.4.2 可兼与不可兼析取命题

汉语中描述析取的连接词很少，主要是“或”和“或者”。

例 1-8 用符号表示下述命题。

(1) 王学东爱听音乐或爱看电影。

(2) 徐燕玲昨天一口气做了 20 或 30 道习题。

解 (1) 可表示为两个原子命题 p 和 q 的析取 $p \vee q$，其中，p：王学东爱听音乐，q：王学东爱看电影。

(2) 这里的“或”表示不确定估计，代表一个模糊的量，视为原子命题更合适。

[辨析] 在遇到联结词“或”时，第一件要做的事不是用符号表示，而是分析它究竟是可兼或还是不可兼或。

例 1-9 用符号表示下述命题。

(1) 马拉松比赛在明天上午 9 点或者下午 2 点举行。

(2) 我要出去看电影或者在家看电视。

(3) 黄渤可能是 100 米赛跑或 400 米赛跑的冠军（每人只限参加一项比赛）。

(4) 黄渤住在 202 或 203 房间。

解 很明显，上述命题中的两个原子命题不能同时为真，或者说，原子命题同时为真时复合命题为假。因此，这些命题均要表示为两个原子命题 p 和 q 的不可兼析取 $p \bar{\vee} q$。从含义或值的角度出发，也可以表示为 $(p \wedge \neg q) \vee (\neg p \wedge q)$，或 $\neg(p \leftrightarrow q)$。

1.4.3 条件命题

汉语中的条件联结词很多，可以归为两类，须注意区分。

例 1-10 用符号表示下述命题。

(1) 因为感染了病毒，所以系统运行不正常。

(2) 只要努力，就一定会成功。

(3) 当山花开的时候，你爹就回来了。

解 若 p 表示前件，分别是：

(1) p：感染了病毒，(2) p：努力，(3) p：山花开了，或 p：到了山花开的时候。

q 表示后件，分别是：

(1) q：系统运行不正常，(2) q：一定会成功，(3) q：你爹回来了。

那么，上述复合命题均可用符号表示为：

$$p \rightarrow q。$$

例 1-11　用符号表示下述命题。

(1) 只有社会主义才能救中国。

(2) 爱拼才会赢。

(3) 仅当你尽了全力，才能打赢这一仗。

(4) 除非你尽了全力，才能打赢这一仗。

(5) 除非你尽了全力，否则不能打赢这一仗。

解　若 p 表示后件，分别是：

(1) p：走社会主义道路，(2) p：爱拼，(3)、(4)、(5) p：你尽了全力。

令 q 表示前件，分别为：

(1) q：救中国，(2) q：会赢，(3)、(4)、(5) q：你打赢这一仗。

那么，上述命题均可用符号表示为：

$$q \rightarrow p。$$

上述两组命题说明了两类条件句的差异，要分清究竟谁是前件，谁是后件，或者说哪个命题是前提，哪个命题才是结论。

用示例来说，其核心问题是强调条件句“只有努力才会成功”与“只要努力就会成功”的不同。第一个命题是正确的，如果成功了，一定经过了努力。第二个陈述是错误的，不是客观事实。因为，即便努力了，但如果方法不正确，或者条件不成熟，也不能保证成功。

又如，在程序设计中，“仅当程序没有任何语法错误，才能运行出正确的结果”与“只有程序没有任何语法错误，才能运行出正确的结果”是相同的描述，但与“只要程序中没有任何语法错误，就能运行出正确的结果”完全不同。因为即使没有语法错误，也可能存在逻辑错误，这种情况下仍得不到正确的运行结果。

[辨析]　“只有、才”与“只要、就”组成条件句时条件与结论恰好相反。只要 p 就 q，表示 p 是 q 的充分条件，符号化为 $p \rightarrow q$；只有 p 才 q，说明 p 是 q 的必要条件，符号化为 $q \rightarrow p$。

[辨析]　“当”与“仅当”的条件与结论恰好相反。“当”与“只要”相同，“仅当”与“只有”同义。“当且仅当”（if and only if，或 iff）是常用的充分必要条件，即互为条件，拆开就是“当”而且“仅当”，“有且只有”是等同的说法。

[辨析]　“除非”（unless）就是“如果不”，其后可以有肯定和否定两种说法，意思相同。直译为 $\neg p \rightarrow \neg q$，等同于 $q \rightarrow p$。

1.4.4　多联结词命题

例 1-12　将下述命题用符号表示。

(1) 我们要做到身体好、学习好、工作好，为祖国四化建设而奋斗。

解　记 p：我们要做到身体好。q：我们要做到学习好。r：我们要做到工作好。s：我们为祖国四化建设而奋斗。命题可形式化为：

$$(p \wedge q \wedge r) \leftrightarrow s。$$

这里采用双条件联结词是考虑了命题的内在联系。如果我们做到了 p、q、r 时就是在为四化建设奋斗，而为四化建设奋斗就是指做到了 p、q、r。

(2) 我没收到他的信。可见，要么他没给我写信，要么信在邮寄途中丢失了。

解 记 p：我没收到他的信。q：他没给我写信。r：信在邮寄途中丢失了。命题可形式化为：

$$p \rightarrow (q \bar{\vee} r)。$$

首先注意到不可兼析取，没写信和信丢失不能同时成立。其次，后面的判断显然是对“没收到信”的前提做的结论。

(3) 假如上午不下雨，我去图书馆，否则就在家里读书或写作业。

解 原命题等同于：假如上午不下雨，我去图书馆；假如上午下雨，就在家里读书或写作业。

这是说话人都认可的两个命题组成的并列句。因此，记 p：上午下雨。q：我去图书馆。r：我在家里读书或写作业。命题可形式化为：

$$(\neg p \rightarrow q) \wedge (p \rightarrow r)。$$

[辨析] 为什么此题目不能表示成不可兼析取 $(\neg p \rightarrow q) \bar{\vee} (p \rightarrow r)$ 呢?

考虑这种情况：上午没下雨，但我没去图书馆。此时，p 为 0，$\neg p$ 为 1，q 为 0。由于违背了原命题，符号化命题的值应为 0。但 $\neg p \rightarrow q$ 为 0，$p \rightarrow r$ 为 1，即 $(\neg p \rightarrow q) \bar{\vee} (p \rightarrow r)$ 的值为 1 而不是 0，显然是不正确的。

类似地，采用不可兼析取来描述对“上午下雨，我没在家读书或写作业。”的情况也是错误的。

[辨析] “我在家里读书或写作业”也可拆分成两个原子命题的析取，可兼、不可兼均可。

(4)人不犯我，我不犯人；人若犯我，我必犯人。

解 记 p：人犯我。q：我犯人。命题可形式化为：

$$(\neg p \rightarrow \neg q) \wedge (p \rightarrow q)。$$

因为以上复合命题是 4 个原子命题组成的并列句，且 p 与 q 互为条件，故也可以直接符号化为：

$$p \leftrightarrow q。$$

(5) 一个人起初说，“占据空间的、有质量的而且不断变化的叫做物质”。后来他改说，“占据空间的有质量的叫做物质，而物质是不断变化的”。符号化这两个命题以反映出二者的差异。

解 记 p：某种东西占据空间。q：某种东西有质量。r：某种东西不断变化。s：某种东西叫做物质。命题可分别形式化为：

$$(p \wedge q \wedge r) \leftrightarrow s,$$

$$(p \wedge q \leftrightarrow s) \wedge (s \rightarrow r)。$$

[辨析] 给一个概念下定义一定是用双条件来形式化的，即“描述 $\leftrightarrow$ 概念”。换言之，此就是彼，且彼就是此。

(6) 如果你来了，那么他唱不唱歌将看你是否伴奏而定。

解　记 p：你来了。q：他唱歌。r：你伴奏。命题可形式化为：

$$p \to (q \leftrightarrow r)。$$

这句话等同于说，他唱歌一定由你伴奏，而你伴奏的话他就唱歌。

思考与练习 1.4

1-20　用符号形式描述下述命题。

(a) 黄渤是青岛人或烟台人。

(b) 选修物联网或嵌入式课，但不同时都选修的学生，可以选修移动互联编程课。

(c) 只有具备工程实践能力的人，才能顺利应付即将面临的工作。

(d) 球队不可能获胜，除非是主场比赛。

(e) 除非你年满 18 周岁，否则，如果你身高不足 1.5 米，就不能参加这次滑雪或游泳比赛。

(f) 为了提高逻辑思维能力，必要条件（但不是充分条件）是认真听讲并勤于思考。

(g) 总吹南风预示着春天就要来了。

(h) 仅当你坚持实际编写和调试程序，才能学会用计算机解决问题。

1-21　设 p：你通过了这门课的测试，q：你做了所有的作业，r：这门课你得了优。用符号表示下述命题：

(a) 这门课你得了优，但你并没有做所有的作业。

(b) 你通过了这门课的测试，你做了所有的作业，且这门课你得了优。

(c) 你想这门课得优，必须通过这门课的测试。

(d) 你通过了这门课的测试，你并没有做所有的作业，但这门课你还是得了优。

(e) 你通过了这门课的测试，又做了所有的作业，足以使你这门课得优。

(f) 你这门课得优，仅当你做了所有的作业或你通过了这门课的测试。

1-22　判断下述命题中的“或”是可兼析取还是不可兼析取，并说明为什么。

(a) 这个工作要求有 C++或 Java 编程经验。

(b) 一次购买此超市的 200 元商品，你可以得到 20%的现金减免或 50 元的代金券。

(c) 出版或销毁。

(d) 雪过大或天气太冷，这里的学校就会停课。

1-23　对位串 0001110001 和 1001001000 分别做按位与（$\wedge$）、或（$\vee$）和异或（$\veebar$）运算的结果是什么？对应的十进制值是多少？

1-24　将自然语言翻译成符号逻辑表达式是硬件系统或软件系统说明的重要内容，目的是生成精确、无二义性的规范说明，构成系统开发的基础。这些规范说明应该是一致的，不应包含有冲突的需求。检查冲突的方法是针对原子变元的所有赋值看命题的真值是否存在矛盾。以下是一个邮件系统的部分规范说明，试符号化并检查是否含有冲突。

(a) 每当邮件来自一个未知的系统时，就扫描邮件中的病毒。
(b) 邮件来自一个未知的系统，但不扫描邮件中的病毒。
(c) 每当邮件来自一个未知的系统时，就有必要扫描邮件中的病毒。
(d) 当邮件不是来自一个未知的系统时，就不扫描邮件中的病毒。

1.5 命题公式的值与等价

1.5.1 命题公式的分类

依据命题公式在不同解释下的真值不同可将命题公式分为 3 类。

[定义 1-14] 假设 A 是一个命题公式。若 A 在所有解释下的真值都为 1，则 A 是**永真式**或**重言式**（tautology）。若 A 在所有解释下的真值都为 0，则 A 是**永假式**或**矛盾式**（contradiction）。若至少存在一个解释使 A 为 1，则 A 是**可满足式**（contingency）。显然，只有永假式是不可满足的。

用函数的观点说，永真式和永假式就是常量函数。无论 p 和 q 表示什么命题，$p \wedge \neg p$、$(p \vee q) \wedge \neg(p \vee q)$ 和 $p \wedge 0$ 都是永假式，$p \vee \neg p$、$(p \to q) \vee \neg(p \to q)$ 和 $p \vee 1$ 都是永真式。

[定理 1-1] 若命题 $A(p_1, p_2, \cdots, p_n)$ 为永真式，那么，分别用命题公式 $q_1, q_2, \cdots, q_n$ 替换 A 中的命题变元 $p_1, p_2, \cdots, p_n$，所得到的公式 $A(q_1, q_2, \cdots, q_n)$ 仍为永真式。

此定理称为“**永真式代入定理**”。永假式也有类似的结论。

因为永真式的真值与命题变元的取值无关，此定理是显然的。例如，命题 $\neg(p \wedge q) \vee (p \wedge q)$ 为永真式，用 q、s 替换 p、q 得到的命题 $\neg(q \wedge s) \vee (q \wedge s)$ 仍为永真式。

1.5.2 命题公式的等价

[定义 1-15] 若命题公式 $A(p_1, p_2, \cdots, p_n)$ 和 $B(p_1, p_2, \cdots, p_n)$ 有相同的原子变元，且对 $p_1, p_2, \ldots, p_n$ 的每个解释，A 和 B 的值都相同，则公式 A 和 B 相等，一般称为 A 和 B **等价**（logical equivalence）或**等值**，记作 $A \Leftrightarrow B$，或 $A \equiv B$。

[辨析] 命题公式等价就是命题函数相等。数学上，函数相等有 3 要素，即定义域相同、值域相同且对应关系相同。很明显，只要两个命题公式 A 和 B 的原子变元一样，其定义域和值域自然相同。因此，只要对应关系相同则二者相等。

若 $A(p_1, p_2, \cdots, p_n) \Leftrightarrow B(p_1, p_2, \cdots, p_n)$，自然有

$$A(\neg p_1, \neg p_2, \cdots, \neg p_n) \Leftrightarrow B(\neg p_1, \neg p_2, \cdots, \neg p_n)。$$

两个公式等价意味着它们有完全相同的真值表。事实上，它们是同一个命题的不同表示，只是因为考虑问题的角度不同而造成了表示上的差异。

除后文的主范式方法外，证明两公式等价主要有 3 种方法：

(1) 真值表法

将两个公式的真值表列出，如果二者完全相同则意味着公式等价。如表 1-4 证明了公式 $p \to q \Leftrightarrow \neg p \vee q$ 和 $p \bar{\vee} q \Leftrightarrow (p \wedge \neg q) \vee (\neg p \wedge q)$。

表 1-4

p	q	$p\to q$	$\neg p\vee q$	$p\bar{\vee}q$	$p\wedge\neg q$	$\neg p\wedge q$	$(p\wedge\neg q)\vee(\neg p\wedge q)$
1	1	1	1	0	0	0	0
1	0	0	0	1	1	0	1
0	1	1	1	1	0	1	1
0	0	1	1	0	0	0	0

［辨析］这是两个十分重要的等价关系，它们体现了将条件和不可兼析取转换为最基本联结词的方法。

利用真值表法很容易验证一些基本的算律，如交换律、结合律、分配律、德·摩根律，参见表 1-5，它们代表了一些最基本的推理定律。

表 1-5

序号	等价关系	含义
E_1	$\neg\neg p\Leftrightarrow p$	对合律（双重否定律）
E_2 E_3	$p\wedge q\Leftrightarrow q\wedge p$ $p\vee q\Leftrightarrow q\vee p$	交换律
E_4 E_5	$(p\wedge q)\wedge r\Leftrightarrow p\wedge(q\wedge r)$ $(p\vee q)\vee r\Leftrightarrow p\vee(q\vee r)$	结合律
E_6 E_7	$p\wedge(q\vee r)\Leftrightarrow(p\wedge q)\vee(p\wedge r)$ $p\vee(q\wedge r)\Leftrightarrow(p\vee q)\wedge(p\vee r)$	分配律
E_8 E_9	$\neg(p\wedge q)\Leftrightarrow\neg p\vee\neg q$ $\neg(p\vee q)\Leftrightarrow\neg p\wedge\neg q$	德• 摩根律（De Morgan）
E_{10} E_{11}	$p\vee p\Leftrightarrow p$ $p\wedge p\Leftrightarrow p$	等幂律
E_{12} E_{13}	$q\vee(p\wedge\neg p)\Leftrightarrow q$ （$q\vee 0\Leftrightarrow q$） $q\wedge(p\vee\neg p)\Leftrightarrow q$ （$q\wedge 1\Leftrightarrow q$）	同一律
E_{14} E_{15}	$q\vee(p\vee\neg p)\Leftrightarrow 1$ （$q\vee 1\Leftrightarrow 1$） $q\wedge(p\wedge\neg p)\Leftrightarrow 0$ （$q\wedge 0\Leftrightarrow 0$）	零律
E_{16} E_{17}	$p\to q\Leftrightarrow\neg p\vee q$ $\neg(p\to q)\Leftrightarrow p\wedge\neg q$	蕴含等值
E_{18}	$p\to q\Leftrightarrow\neg q\to\neg p$	假言易位
E_{19}	$p\to(q\to r)\Leftrightarrow(p\wedge q)\to r$	
E_{20}	$p\leftrightarrow q\Leftrightarrow(p\to q)\wedge(q\to p)$	等价等值
E_{21} E_{22}	$p\leftrightarrow q\Leftrightarrow(p\wedge q)\vee(\neg p\wedge\neg q)$ $\neg(p\leftrightarrow q)\Leftrightarrow p\leftrightarrow\neg q$	
E_{23}	$p\leftrightarrow q\Leftrightarrow\neg p\leftrightarrow\neg q$	等价否定等值
E_{24}	$(p\to q)\wedge(p\to\neg q)\Leftrightarrow\neg p$	归谬论
E_{25} E_{26}	$p\bar{\vee}q\Leftrightarrow\neg(p\leftrightarrow q)$ $p\bar{\vee}q\Leftrightarrow(p\wedge\neg q)\vee(\neg p\wedge q)$	

(2) 等价变换法

如果一个公式中的某个部分仍是命题公式，一般称其为原公式的“**子公式**”。很明显，有：

定理[1-2] 设 X 是命题公式 A 的子公式，且 $X \Leftrightarrow Y$。若在 A 中用 Y 部分或全部替换 X 得到命题公式 B，则 $A \Leftrightarrow B$。

换言之，利用对命题公式本身或它的子公式进行等价替换不改变原公式的值。此定理被称为“（等价）置换规则”。

例 1-13 证明 $p \to (q \to r) \Leftrightarrow q \to (p \to r)$。

证明
$$\begin{aligned} p \to (q \to r) &\Leftrightarrow_{(\text{原公式等价变换})} \neg p \vee (q \to r) \\ &\Leftrightarrow_{(\text{子公式等价变换})} \neg p \vee (\neg q \vee r) \\ &\Leftrightarrow_{(\text{交换律、结合律})} \neg q \vee (\neg p \vee r) \\ &\Leftrightarrow_{(\text{子公式和原公式等价变换})} q \to (p \to r)。 \end{aligned}$$

上述等价变换与 $a+(b+c)^2 = a+(b^2+2bc+c^2)$、$a-(-b+c) = a-(c-b)$ 没有什么不同，就是等值演算。

例 1-14 证明对任意命题公式 p 和 q，有

$$p \uparrow p \Leftrightarrow \neg p, (p \uparrow p) \uparrow (q \uparrow q) \Leftrightarrow p \vee q, (p \uparrow q) \uparrow (p \uparrow q) \Leftrightarrow p \wedge q,$$
$$p \downarrow p \Leftrightarrow \neg p, (p \downarrow p) \downarrow (q \downarrow q) \Leftrightarrow p \wedge q, (p \downarrow q) \downarrow (p \downarrow q) \Leftrightarrow p \vee q。$$

证明 仅验证↑，有

$$p \uparrow p \Leftrightarrow \neg(p \wedge p) \Leftrightarrow \neg p,$$
$$(p \uparrow p) \uparrow (q \uparrow q) \Leftrightarrow \neg p \uparrow \neg q \Leftrightarrow \neg(\neg p \wedge \neg q) \Leftrightarrow p \vee q,$$
$$(p \uparrow q) \uparrow (p \uparrow q) \Leftrightarrow \neg(p \uparrow q) \Leftrightarrow \neg(\neg p \vee \neg q) \Leftrightarrow p \wedge q。$$

验证中采用了表 1-5 中的德·摩根律和双重否定律。

由上述等价关系可以看出，联结词↑和↓均可用 $\neg$、$\wedge$、$\vee$ 来表示。

(3) 双条件式永真法

[定理 1-3] 对于命题公式 p 和 q，$p \Leftrightarrow q$ 当且仅当 $p \leftrightarrow q$ 为永真式。

因为 $p \leftrightarrow q$ 只在 p 与 q 具有相同值时为真，结论是显然的。

[辨析] 这是一个需要熟记的结论，可以作为“命题公式等价的判定定理”。

由于 $p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)$，上述定理也可叙述为：

$p \Leftrightarrow q$ 当且仅当 $p \to q$ 和 $q \to p$ 均为永真式。

例 1-15* 化简下述 C 语言程序：

if (p) { **if** (q) statement1; **else** statement2; } **else** { **if** (q) statement1; **else** statement2; }

解 statement1 的执行需满足条件

$$(p \wedge q) \vee (\neg p \wedge q) \Leftrightarrow (p \vee \neg p) \wedge q \Leftrightarrow q。$$

statement2 的执行需满足条件

$$(p \wedge \neg q) \vee (\neg p \wedge \neg q) \Leftrightarrow (p \vee \neg p) \wedge \neg q \Leftrightarrow \neg q。$$

因此，程序可简化为：

if (q) statement1; **else** statement2;

1.5.3　联结词的功能完备集

为什么定义 9 个联结词呢？我们不妨列出 2 个命题变元在不同赋值下所有可能的命题真值，参见表 1-6。

因为 2 个原子变元的命题共有 4 种解释，而对应每个解释，命题的真值有 2 种可能，故共有 2^4 种可能。该表说明，9 个联结词组成的联结词集合是**联结词的功能完备集**（complete group of connectives，或**全功能联结词组**）。联结词功能完备集就是指任何命题都可以由此集合中的联结词表示出来。

表 1-6

p	q	1	0	p	q	$\neg p$	$\neg q$	$p \wedge q$	$p \uparrow q$
1	1	1	0	1	1	0	0	1	0
1	0	1	0	1	0	0	1	0	1
0	1	1	0	0	1	1	0	0	1
0	0	1	0	0	0	1	1	0	1
p	q	$p \vee q$	$p \downarrow q$	$p \to q$	$p \overset{c}{\to} q$	$p \leftrightarrow q$	$p \bar{\vee} q$	$q \to p$	$q \overset{c}{\to} p$
1	1	1	0	1	0	1	0	1	0
1	0	1	0	0	1	0	1	1	0
0	1	1	0	1	0	0	1	0	1
0	0	0	1	1	0	1	0	1	0

事实上，将某些联结词用其他联结词等价表示可以有效地减少联结词的数目。例如，考虑如下等价关系：

$$p \to q \Leftrightarrow \neg p \vee q\,,\quad p \overset{c}{\to} q \Leftrightarrow \neg(p \to q)\,,$$

$$p \bar{\vee} q \Leftrightarrow \neg(p \leftrightarrow q)\,,\quad p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)\,,$$

$$p \uparrow q \Leftrightarrow p \wedge q\,,\quad p \downarrow q \Leftrightarrow p \vee q\,。$$

这说明，联结词$\to$、$\leftrightarrow$、$\overset{c}{\to}$、$\bar{\vee}$、$\uparrow$、$\downarrow$均可由$\neg$、$\vee$、$\wedge$表示，故$\{\neg,\wedge,\vee\}$是功能完备的。又由例 1-14 可知，联结词$\neg$、$\wedge$、$\vee$可用$\uparrow$来表示，也可用$\downarrow$来表示，说明$\{\uparrow\}$和$\{\downarrow\}$也都是联结词功能完备集。从联结词数量上看，这是两个最小的联结词功能完备集。

能够用极少的联结词描述所有命题意味着，可以采用种类单一的逻辑元器件设计出任何复杂的逻辑电路，从而降低制作工艺的复杂性，这是制作大规模集成电路的理论基础。

1.5.4　由德·摩根律到对偶原理

表 1-5 中列出的德·摩根律是命题演算中的最基本运算律之一，体现了如下的命题等价关系：

$$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q,\ \neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q。$$

这种公式都是成对的，且变元也常常不止 2 个。不妨想象一下如下公式的情形：

$$\neg((p \wedge q) \vee r) \Leftrightarrow ?，\neg((p \vee q) \wedge r) \Leftrightarrow ?$$

由于{┐，∧，∨}是联结词的功能完备集，即任何命题都可由这 3 个联结词表示，由此可将德• 摩根律推广到更一般的形式，即对偶原理。

[定义 1-16] 将一个命题公式 A 中所有∧换成∨，∨换成∧，1 换成 0，0 换成 1，得到的命题公式 A^*称为 A 的**对偶式**。当然，A 也是 A^*的对偶式，即 A 和 A^*互为对偶。

由定义可知，1 与 0 互为对偶式，$(p \wedge q) \vee r$ 与 $(p \vee q) \wedge r$ 互为对偶式。因为 $p \uparrow q \Leftrightarrow \neg(p \wedge q)$，$p \downarrow q \Leftrightarrow \neg(p \vee q)$，故 $p \uparrow q$ 与 $p \downarrow q$ 互为对偶式。

[辨析] *求对偶式与否定┐没有任何关联!*

若记 $A(p,q) = p \wedge q$，其对偶式 $A^*(p,q) = p \vee q$，再看德• 摩根律就是

$$\neg A(p,q) \Leftrightarrow \neg p \vee \neg q \Leftrightarrow A^*(\neg p, \neg q)。$$

上述公式中仅有 2 个变元，增加一些变元后就得到了著名的对偶原理。

[定理 1-4] 设命题公式 A 和 A^*是对偶式，p_1，p_2，...，p_n 是公式中包含的原子变元，则

$$\neg A(p_1, p_2, \cdots, p_n) \Leftrightarrow A^*(\neg p_1, \neg p_2, \cdots, \neg p_n)。$$

定理中的等式主要体现的问题是原子变元可能多于 2 个，是推广的德 • 摩根律，称为**对偶原理**（duality principle）。

上述定理可以改换成其他写法。例如，对哪个公式的原子变元否定都可以，因为是相互的：

$$\neg A(\neg p_1, \neg p_2, \cdots, \neg p_n) \Leftrightarrow A^*(p_1, p_2, \cdots, p_n)。$$

可以对等价式两边的任何一个公式做否定：

$$A(p_1, p_2, \cdots, p_n) \Leftrightarrow \neg A^*(\neg p_1, \neg p_2, \cdots, \neg p_n)。$$

这说明了一个明显的事实：同一个公式不可能有两个不一样的对偶式，即

[定理 1-5] 若 $A \Leftrightarrow B$，则 $A^* \Leftrightarrow B^*$。

证明：因为 $A \Leftrightarrow B$，由前文对等值式的讨论，有 $A(\neg p_1, \neg p_2, \cdots, \neg p_n) \Leftrightarrow B(\neg p_1, \neg p_2, \cdots, \neg p_n)$。于是，有：

$$\neg A(\neg p_1, \neg p_2, \cdots, \neg p_n) \Leftrightarrow \neg B(\neg p_1, \neg p_2, \cdots, \neg p_n)$$

即 $A^* \Leftrightarrow B^*$。

对此定理的另一种解释是，两个公式等值则它们的对偶式等值。

思考与练习 1.5

1-25 解释命题等价、蕴含的含义以及二者的关系。

1-26 命题公式分为几种类型？各有什么特点？

1-27 证明 $((p \to q) \wedge (q \to r)) \to (p \to r)$ 是永真式。

1-28　证明下述等价公式：

(a) $\neg p \to (q \to r) \Leftrightarrow q \to (p \vee r)$。　(b) $p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)$。

(c) $\neg(p \leftrightarrow q) \Leftrightarrow p \leftrightarrow \neg q$。

1-29　求下述公式的对偶式：

(a) $p \wedge (q \vee (r \wedge 1))$。　(b) $\neg p \to (q \to r)$。

(c) $(p \bar{\vee} q) \uparrow r$。

1-30　若 p、q 和 r 为命题变元，证明或否定：

(a) 如果 $p \wedge q \Leftrightarrow p \wedge r$，则 $q \Leftrightarrow r$。　(b) 如果 $p \vee q \Leftrightarrow p \vee r$，则 $q \Leftrightarrow r$。

(c) 如果 $\neg q \Leftrightarrow \neg r$，则 $q \Leftrightarrow r$。　(d) 如果 $p \bar{\vee} q \Leftrightarrow p \bar{\vee} r$，则 $q \Leftrightarrow r$。

1-31　记 A^* 是公式 A 的对偶式，何时有 $A^* \Leftrightarrow A$？

1-32　记 A^* 是公式 A 的对偶式，证明 $(A^*)^* \Leftrightarrow A$。

1-33　证明{$\neg$、$\wedge$}、{$\neg$、$\to$}和{$\neg$、$\overset{c}{\to}$}是联结词的功能完备集。

1.6　范　　式

任意给定 2 个命题公式，它们的值相等吗？或者说，它们描述的是同一个命题吗？除了采用列真值表和置换规则等方法外，还有一种重要的判别方法是将公式转换成标准形式后再进行比较，这种标准形式称为“**范式**”（normal form）。

由于{$\neg, \wedge, \vee$}是联结词的功能完备集，利用等价关系、置换规则、对偶原理等去掉其他联结词，就得到了只有$\neg$、$\wedge$、$\vee$的命题公式，进而可以将其转换为范式，就是“标准型”。

1.6.1　简单的范式

为了使叙述简单，先明确一种说法。

[定义 1-17] 原子命题变元或它的否定称为**文字**。如 p 和 $\neg p$、q 或 $\neg q$。

[定义 1-18] 一个命题公式称为**合取范式**，如果它具有形式：

$$A_1 \wedge A_2 \wedge \cdots \wedge A_n,\quad n \geqslant 1。$$

其中，每个 A_i 都是由文字组成的析取式。

一个命题公式称为**析取范式**，如果它具有形式：

$$A_1 \vee A_2 \vee \cdots \vee A_n,\quad n \geqslant 1。$$

其中，每个 A_i 都是由文字组成的合取式。

例如，$(p \vee \neg q \vee r) \wedge (\neg p \vee q) \wedge \neg q$ 为合取范式，$\neg p \vee (p \wedge q) \vee (p \wedge \neg q \wedge r)$ 是析取范式。

还可以换个说法，称合取范式为“积范式”，可记作 $\prod_{i=1}^{n} A_i$。称析取范式为“和范式”，可记作 $\sum_{i=1}^{n} A_i$。合取或析取代表最终的运算。

[辨析] 单个文字如 p 和 $\neg p$ 既是合取范式，也是析取范式，相当于定义中的 n=1，A_1=p，或 A_1=$\neg p$。

[辨析] 单个合取式或析取式既是合取范式，也是析取范式。例如，合取式 $p \wedge \neg q$，说它是合取范式，相当于定义中的 $n=2, A_1=p, A_2=\neg q$。说它是析取范式，相当于定义中的 $n=1, A_1=p \wedge \neg q$。

[辨析] 定义 1-18 不够严格，没有限制文字的重复性，永真式 $1 \Leftrightarrow p \vee \neg p$ 既是合取范式，也是析取范式。永假式 $0 \Leftrightarrow p \wedge \neg p$ 既是合取范式，也是析取范式。

应特别注意的是，否定只能作用在原子变元前，不能置于括号前。

通过等价演算可以很容易按下述步骤求得一个命题公式的范式：

(1) 联结词转换为 $\wedge$、$\vee$ 及 $\neg$；

(2) 用德·摩根律（对偶原理）将否定符号 $\neg$ 直接作用到各原子变元之前；

(3) 用分配律、结合律和交换律等归约为合取范式或析取范式。

例 1-16 求 $(p \wedge (q \rightarrow r)) \rightarrow s$ 的合取范式。

解
$$(p \wedge (q \rightarrow r)) \rightarrow s \Leftrightarrow_{(\text{规范联结词})} \neg(p \wedge (\neg q \vee r)) \vee s$$
$$\Leftrightarrow_{(\text{否定深入})} \neg p \vee (q \wedge \neg r) \vee s$$
$$\Leftrightarrow_{(\text{分配律、交换律、结合律})} (\neg p \vee s \vee q) \wedge (\neg p \vee s \vee \neg r)。$$

一个命题公式的合取范式与析取范式并不唯一。例如，对于一个合取范式 $A=p$，有

$$A \Leftrightarrow p \vee (q \wedge \neg q) \Leftrightarrow (p \vee q) \wedge (p \vee \neg q)。$$

这说明简单范式并不标准。原因是对定义中的 A_i 要求不严格，结果的形式不唯一。一个公式如文字还可以既是析取范式也是合取范式，含有歧义。

1.6.2 小项与大项

[定义 1-19] n 个命题变元的合取式称为（**极**）**小项**或**布尔合取**（minimal term），如果它包含每个变元的文字一次且仅一次。

例如，一个命题变元的小项为 p 和 $\neg p$，两个命题变元的小项为 $p \wedge q$、$p \wedge \neg q$、$\neg p \wedge q$、$\neg p \wedge \neg q$。一般地，n 个命题变元有 2^n 个小项。

由于只有一种解释使每个小项为 1，可用此解释对应的二进制串作为对该小项的编码（起个独特的名字）。如：

$$m_{11}=p \wedge q，\ m_{10}=p \wedge \neg q，\ m_{01}=\neg p \wedge q，\ m_{00}=\neg p \wedge \neg q。$$

写成十进制更简单，还容易看清楚：

$$m_3=p \wedge q，\ m_2=p \wedge \neg q，\ m_1=\neg p \wedge q，\ m_0=\neg p \wedge \neg q。$$

很明显，对于每个小项，只有变元取值与其二进制编码相同时才为 1，其余全为 0。同时，对原子变元的任何一个解释，必能使一个且仅一个小项为 1，其余全为 0，即任意 2 个小项不能同时为 1。于是，对任意不同的 i，j，有：

(1) $m_i \wedge m_j=0$，$0 \leqslant i \neq j \leqslant 2^n-1$；

(2) $\sum_{i=0}^{2^n-1} m_i=1$。

[定义 1-20] n 个命题变元的析取式称为（**极）大项**或**布尔析取**（maximal term），如果它包含每个变元的文字一次且仅一次。

例如，一个命题变元的大项为 p 和 $\neg p$，两个命题变元的大项为 $p \vee q$、$p \vee \neg q$、$\neg p \vee q$、$\neg p \vee \neg q$。一般地，n 个命题变元有 2^n 个大项。

由于每个大项只有一种解释使其为 0，也可用此解释对应的二进制串作为对它的编码。如：

$M_0 = M_{00} = p \vee q$，$M_1 = M_{01} = p \vee \neg q$，$M_2 = M_{10} = \neg p \vee q$，$M_3 = M_{11} = \neg p \vee \neg q$。

对于每个大项，只有变元取值与其二进制编码相同时才为 0，其余全为 1。同时，对原子变元的任何一组解释，必能使一个且仅一个大项为 0，其余全为 1，即 2 个大项不能同时为 0。于是，对任意不同的 i，j，有

(1) $M_i \vee M_j = 1$，$0 \leqslant i \neq j \leqslant 2^n - 1$；

(2) $\prod_{i=0}^{2^n-1} M_i = 0$。

[辨析] 为什么叫做小项？值小，求积几乎总是 0。为什么叫做大项？值大，求和几乎总是 1。

[定理 1-6] 对任意的 i，$0 \leqslant i \leqslant 2^n - 1$，有

$$\neg m_i \Leftrightarrow M_i，\quad \neg M_i \Leftrightarrow m_i。$$

用 2 个变元演示一下可一目了然，如：

$$\neg m_2 = \neg m_{10} = \neg(p \wedge \neg q) = \neg p \vee q = M_{10} = M_2。$$

上述结论来源于对小项和大项的编码技术，能够正确地写出这些编码是至关重要的。

如何将普通合取式和析取式分别转换为小项或大项呢？方法是添加与 1 的合取，或与 0 的析取，将 1 和 0 用缺少的变元替换，再加上分配律就可以了。

例如，对于 3 个变元 p、q 和 r，公式 $A = p \wedge \neg q$ 是合取式，但不是小项，缺少 r。于是，应按如下方式进行等价变换：

$$\begin{aligned} A = p \wedge \neg q &\Leftrightarrow (p \wedge \neg q) \wedge 1 \Leftrightarrow (p \wedge \neg q) \wedge (r \vee \neg r) \\ &\Leftrightarrow (p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r)。\end{aligned}$$

这就将 A 转换成了 2 个小项的析取。

1.6.3　主析取范式与主合取范式

[定义 1-21] 仅由小项的析取所组成的命题公式称为**主析取范式**（major disjunctive form），仅由大项的合取所组成的命题公式称为**主合取范式**（major conjunctive form）。

通常，主析取范式 $m_{i_1} \vee m_{i_2} \vee \cdots \vee m_{i_t}$ 简记为 $\Sigma_{i_1,i_2,\cdots,i_t}$ 或 $\Sigma_{\{i_1,i_2,\cdots,i_t\}}$，主合取范式 $M_{i_1} \wedge M_{i_2} \wedge \cdots \wedge M_{i_t}$ 简记为 $\Pi_{i_1,i_2,\cdots,i_t}$ 或 $\Pi_{\{i_1,i_2,\cdots,i_t\}}$。

由于前文已经演算过析取范式和合取范式，得到主析取范式和主合取范式只差一个添加缺少原子变元的步骤了。

例 1-17　求 $p \to ((p \to q) \wedge \neg(\neg q \vee \neg p))$ 的主析取范式和主合取范式。

解　原式 $\Leftrightarrow \neg p \vee ((\neg p \vee q) \wedge (q \wedge p))$

$\Leftrightarrow \neg p \vee ((\neg p \wedge q \wedge p) \vee (q \wedge q \wedge p))$

$\Leftrightarrow \neg p \vee (p \wedge q)$ 注：析取范式

$\Leftrightarrow (\neg p \wedge (q \vee \neg q)) \vee (p \wedge q)$ 注：在缺 q 的项上添加 $1 = q \vee \neg q$

$\Leftrightarrow (\neg p \wedge q) \vee (\neg p \wedge \neg q) \vee (p \wedge q)$ 注：利用分配律得到主析取范式

$= m_{01} \vee m_{00} \vee m_{11}$

$= \Sigma_{\{0,1,3\}}$。

原式 $\Leftrightarrow \neg p \vee ((\neg p \vee q) \wedge (q \wedge p))$

$\Leftrightarrow \neg p \vee (p \wedge q) \Leftrightarrow 1 \wedge (\neg p \vee q) \Leftrightarrow \neg p \vee q$ 注：利用分配律得到主合取范式

$= M_{10}$

$= \Pi_{\{2\}}$。

例 1-18 求 $(p \vee q \vee r) \wedge (\neg p \vee r)$ 的主合取范式。

解 原式 $\Leftrightarrow (p \vee q \vee r) \wedge (\neg p \vee r \vee (q \wedge \neg q))$ 注：在缺 q 的项上添加 $0 = q \wedge \neg q$

$\Leftrightarrow (p \vee q \vee r) \wedge (\neg p \vee q \vee r) \wedge (\neg p \vee \neg q \vee r)$

$= M_{000} \wedge M_{100} \wedge M_{110}$

$= \Pi_{\{0,4,6\}}$。

一旦变元数量较多，这种添 1 或 0 再加分配律的等价变换办法很烦琐，而使用真值表可以不必经过演算直接求得主合取范式和主析取范式。

[定理 1-7] 在任意命题公式 A 的真值表中，所有使其值为 1 的解释作编码对应的小项的析取是 A 的主析取范式，所有使其值为 0 的解释作编码对应的大项的合取是 A 的主合取范式。

证明 设使 A 为 1 的解释对应的所有小项为 m_{i_1}、m_{i_2}、$\ldots m_{i_k}$。记 $B = \Sigma_{\{i_1, i_2, \ldots, i_k\}}$，则 $A \Leftrightarrow B$。这是因为，若某个解释使 A 为 1，则对应的小项在 B 中，B 也为 1。若某个解释使 A 为 0，则 B 中的小项都为 0，故 B 为 0。因此，A 与 B 等价，即 B 是 A 的主析取范式。主合取范式的证明类似。

表 1-7 为命题公式 $A = p \rightarrow ((p \rightarrow q) \wedge \neg(\neg q \vee \neg p))$ 的真值表。由真值表知，使公式 A 为 1 的解释是 00、01 和 11，故其主析取范式为：

$$m_{00} \vee m_{01} \vee m_{11} = \Sigma_{\{0,1,3\}}。$$

因为使公式 A 为 0 的解释是 10，故主合取范式为 $M_{10} = \Pi_{\{2\}}$。

表 1-7

p	q	$p \rightarrow q$	$\neg q \vee \neg p$	$(p \rightarrow q) \wedge \neg(\neg q \vee \neg p)$	A	m 或 M
0	0	1	1	0	1	m_{00}
0	1	1	1	0	1	m_{01}
1	0	0	1	0	0	M_{10}
1	1	1	0	1	1	m_{11}

在真值表中，去掉使公式值为 1 的解释，剩下的不就是使公式为假的解释吗？当然。上述公式中，大小项共 4 个，编码为 0~3，主析取范式使用了 0、1、3，主合取范式则使用了剩余的 2。这并不是偶然的巧合。

[定理 1-8] 若公式 A 的主析取范式为 $\Sigma_{\{i_1,i_2,\cdots,i_k\}}$，则主合取范式为 $\Pi_{\{0,1,\cdots,2^n-1\}-\{i_1,i_2,\cdots,i_k\}}$。反之亦然。

证明　若 $A=\Sigma_{\{i_1,i_2,\cdots,i_k\}}$，因 A 与 $\neg A$ 的值相反，故

$$\neg A=\Sigma_{\{0,1,\cdots,2^n-1\}-\{i_1,i_2,\cdots,i_k\}}$$

于是，有

$$A\Leftrightarrow\neg\neg A=\neg\Sigma_{\{0,1,\cdots,2^n-1\}-\{i_1,i_2,\cdots,i_k\}}$$

在对等号右端的公式取非后，$\wedge$ 与 $\vee$ 互换，使 Σ 转换为 Π，且因为 $\neg m_i\Leftrightarrow M_i$，故结论成立。

定理说明，只要知道了一种主范式，用剩余的编码就得到了另一种主范式。例如，若 3 个变元的命题公式（主析取范式）$A=\Sigma_{\{2,5\}}$，那么，A 的主合取范式就是 $\Pi_{\{0,1,3,4,6,7\}}$。

还可以进一步肯定一个事实：

[定理 1-9] 任一命题公式的主析取范式和主合取范式都存在且唯一。这被称为**范式存在定理**。

上述定理成立依赖于对永真式和永假式的特别约定。显然，对于一个含有 n 个命题变元的永真式，其主析取范式为所有小项的析取 $\Sigma_{\{0,1,2,\cdots,2^n-1\}}$，但因为没有使公式为 0 的解释，其主合取范式不包含任何大项，故称为**空范式**，也可说成没有范式，约定用 1 表示。类似地，一个永假式的主合取方式为 $\Pi_{\{0,1,2,\cdots,2^n-1\}}$，其主析取范式为空范式，用 0 表示。

［辨析］主析取范式和主合取范式唯一吗？只要按着编码由小到大或由大到小排列小项和大项就唯一了。

利用范式可以解决一些具有有限约束情况的判定问题。

例 1-19　有一次竞赛，要求在 p、q、r 和 s 这 4 人中指派两人参加，但必须满足如下条件：

(1) p 和 q 仅一个人参加；　　(2) 若 r 参加，则 s 也参加；

(3) q 和 s 至多参加一人；　　(4) 若 s 不参加，则 p 也不参加。

问应如何指派？

解　令 p、q、r 和 s 分别表示命题 p 参加、q 参加、r 参加和 s 参加，则约束条件可符号化为：

$$C=(p\bar{\vee}q)\wedge(r\rightarrow s)\wedge\neg(q\wedge s)\wedge(\neg s\rightarrow\neg p)。$$

计算命题公式 C 的主析取范式为：

$$C=m_{0100}\vee m_{1001}\vee m_{1011}。$$

由于哪个 m_i 为 1 都能保证条件 C 被满足，故每个 m_i 都代表一种可能的选择。不过，根据题目要求，需要指派 2 人参加，故只有 $m_{1001}=p\wedge\neg q\wedge\neg r\wedge s$ 是正确的选派方式，即派 p 和 s 参加。

也可以通过演算将 C 转化为一般的析取范式，再根据题目要求分析得到结果。为了简化，可以在演算过程中不断剔除不满足要求的合取式。

思考与练习 1.6

1-34　说明析取范式、合取范式、主析取范式、主合取范式的含义。

1-35 3 个命题变元组成的公式 $(p\vee\neg q\vee r)\wedge(\neg p\vee q\vee\neg r)$ 的主析取范式是什么？

1-36 任意两个小项组成的合取式的值是什么？任意两个大项组成的析取式的值是什么？

1-37 永真式与永假式的主合取范式与主析取范式各是什么？

1-38 求下述公式的析取范式和合取范式。

(a) p。 (b) $p\vee\neg q$。

(c) $p\wedge r$。 (d) $p\wedge(p\to q)$。

(e) $(\neg p\wedge q)\to r$。 (f) $\neg(p\wedge q)\wedge(\neg p\to q)$。

1-39 分别利用等价演算与真值表计算下述公式的主析取范式和主合取范式。

(a) $(\neg p\wedge q)\wedge(q\to p)$。 (b) $(\neg p\vee\neg q)\to(p\leftrightarrow q)$。

(c) $(\neg p\vee q)\to r$。 (d) $(p\vee(q\wedge r))\to(p\vee q\vee r)$。

1-40 利用主析取范式和主合取范式如何判断公式的类型？根据你的回答计算并判断公式 $(p\to q)\vee(q\to r)\to(p\vee q\to r)$ 的类型。

1-41 若有 4 条指令，分别记作 p、q、r 和 s。一个应用中要选择执行其中的两条指令，但有如下制约条件：

(a) 若执行 p，则 r 和 s 中只能执行一个； (b) q 和 r 不能都执行；

(c) 若执行 r 则不能执行 s。

问共有几种执行指令的方案？各是什么？

1-42 汤姆说珍妮在说谎，珍妮说佛洛依德在说谎，佛洛依德说汤姆、珍妮都在说谎。究竟谁说谎，谁说真话？

1.7 推 理 理 论

从假设前提利用推理规则得到其他命题，即形成结论的过程就是推理，这是研究逻辑的主要目标。

1.7.1 蕴含与论证

1．推理的含义与形式

[定义 1-22] 当且仅当 $p\to q$ 为永真式时，称为 p **蕴含** q（logical implication），记作 $p\Rightarrow q$，或 $p\vdash q$。此时，称 p 为前提，q 为 p 的**有效结论**或**逻辑结论**，也称为 q 可由 p **逻辑推出**。得出此逻辑关系的过程称为**论证**。

[辨析] 由于仅在 p 为 1 而 q 为 0 时公式 $p\to q$ 为 0，可见，$p\to q$ 永真意味着不可能存在前件 p 为 1 而后件 q 为 0 的情况，或者说，若 $p\Rightarrow q$，则只要前件 p 为 1，后件 q 也一定为 1。

所有逻辑推理的实质就是证明 $p\Rightarrow q$，也就是证明 $p\to q$ 为永真式。例如，以下是一个简单的初等数学证明题目：

已知 a、b、c 为实数，且 $a^2-b^2=bc$，$c\neq 0$，证明 $a^2/c=b(b/c+1)$。

如果记

$$p\text{：}\ a^2-b^2=bc\text{，}\ q\text{：}\ c\neq 0\text{，}\ r\text{：}\ a^2/c=b(b/c+1)\text{，}$$

则上述论证要求可描述为：

$$p\wedge q\Rightarrow r\text{。}$$

证明的目的就是说明：若前提 $p\wedge q$ 正确，则结论 r 也正确，即证明 $p\wedge q\to r$ 为永真式。

通常的逻辑推理问题都会由一组前提来推断一个逻辑结论，此时的多个前提可写成合取式 $H_1\wedge H_2\wedge\cdots\wedge H_n$，或写成用逗号分隔的命题序列 $H_1, H_2, ..., H_n$，即论证要求可写作：

$$H_1\wedge H_2\wedge\cdots\wedge H_n\Rightarrow C\text{，或}\ H_1,H_2,...,H_n\Rightarrow C\text{，或}$$

$$H_1\wedge H_2\wedge\cdots\wedge H_n\vdash C\text{，或}\ H_1,H_2,...,H_n\vdash C\text{。}$$

可见，论证 $A\vdash C$ 、$A\Rightarrow C$ 或 $A\to C$ 是永真式都是同义的。

2．常规的推理方法

在日常生活和科学实践中，可以采用一些形式不太严格的方法进行推理论证。

(1) 真值表法，即列出公式 $H_1\wedge H_2\wedge\cdots\wedge H_n\to C$ 的真值表。若公式中所有行的真值全为 1 则得证。这种证明方法没有什么逻辑味道，在命题变元较多时也很困难。

(2) 叙述型推理，说明不存在 $H_1\wedge H_2\wedge\cdots\wedge H_n$ 为 1 且 C 为 0 的情况。可以有两种叙述形式：

① 假定前提 $H_1\wedge H_2\wedge\cdots\wedge H_n$ 为 1，说明结论 C 必为 1。

② 假定结论 C 为 0，说明前提 $H_1\wedge H_2\wedge\cdots\wedge H_n$ 必为 0。

例 1-20　证明 $\neg q\wedge(p\to q)\Rightarrow\neg p$。

证明　这里采用形式①。假定前件 $\neg q\wedge(p\to q)$ 为 1。那么，$\neg q$ 和 $p\to q$ 都为 1。由前者知 q 为 0，再由后者知 p 为 0，故 $\neg p$ 为 1。结论成立。

若采用形式②，可论证如下：

假定后件 $\neg p$ 为 0。于是，p 为 1。

若 q 为 1，则 $\neg q$ 为 0，故 $\neg q\wedge(p\to q)$ 为 0。

若 q 为 0，则 $p\to q$ 为 0，故 $\neg q\wedge(p\to q)$ 为 0。

总之，前件 $\neg q\wedge(p\to q)$ 为 0。结论成立。

例 1-21　用符号描述推理过程并验证论证的有效性：如果 6 是偶数，则 7 被 2 除不尽。或 5 不是素数，或 7 可被 2 除尽。但 5 是素数。所以 6 是奇数。

解　记 p：6 是偶数，q：7 可被 2 除尽，r：5 是素数，则推理过程可符号化为：

$$p\to\neg q,\ \neg r\vee q,\ r\Rightarrow\neg p\text{。}$$

假定前提为 1，则 $p\to\neg q$，$\neg r\vee q$ 和 r 都为 1。由 r 为 1 知 $\neg r$ 为 0，从而 q 为 1。因此，$\neg q$ 为 0，再由 $p\to\neg q$ 为 1 可知 p 为 0。于是，$\neg p$ 为 1。论证有效。

[辨析] 论证有效并不代表结论是客观真实的，因为我们并不研究前提是否具有客观真实性，仅假定其逻辑意义为真，从而进行形式上的推导。

(3) 等值演算，利用等价变换说明条件式为永真式。例如，通过演算可推出

$$((p \to \neg q) \wedge p) \to \neg q \Leftrightarrow 1。$$

这说明 $((p \to \neg q) \wedge p) \Rightarrow \neg q$。

(4) 主析取范式法，即说明条件式的主析取范式包含所有的小项。例如，因为

$$((p \to \neg q) \wedge p) \to \neg q \Leftrightarrow \Sigma_{0,1,2,3} \Leftrightarrow 1。$$

说明 $((p \to \neg q) \wedge p) \Rightarrow \neg q$。

应注意条件式的非对称性。一般称 $q \to p$ 为 $p \to q$ 的**逆换式**（逆命题），称 $\neg p \to \neg q$ 为 $p \to q$ 的**反换式**（反命题），它们均不等同于 $p \to q$。称 $\neg q \to \neg p$ 为 $p \to q$ 的**逆反式**（逆否命题），且有

$$p \to q \Leftrightarrow \neg q \to \neg p。$$

由此可见，如果一个命题成立，其逆否命题也成立。反之亦然。

3．等价与蕴含的关系

由 $p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)$ 可知，蕴含和等价之间有与条件式和双条件式之间类似的关系：

[定理 1-10] 对任意的命题公式 p 和 q，$p \Leftrightarrow q$ 的充分必要条件是 $p \Rightarrow q$ 且 $q \Rightarrow p$。

证明 $p \Leftrightarrow q$ 等同于 $p \leftrightarrow q$ 为永真式，等同于 $(p \to q) \wedge (q \to p)$ 为永真式，等同于 $p \to q$ 和 $q \to p$ 都是永真式，也就等同于 $p \Rightarrow q$ 且 $q \Rightarrow p$。

[辨析] 此定理是应该熟悉的基本逻辑常识，在逻辑证明中常用，也提供了一种证明命题公式等价的方法。

例 1-22 设 p、q、r 是任意命题公式，证明：

(1) 若 $p \Rightarrow q$ 且 p 是永真式，则 q 为永真式。

(2) 若 $p \Rightarrow q$ 且 $q \Rightarrow r$，则 $p \Rightarrow r$。

(3) 若 $p \Rightarrow q$ 且 $p \Rightarrow r$，则 $p \Rightarrow q \wedge r$ 且 $p \Rightarrow q \vee r$。

(4) 若 $p \Rightarrow r$ 且 $q \Rightarrow r$，则 $p \vee q \Rightarrow r$。

证明 (1)、(2)略。

(3) 由条件知，$p \to q$ 和 $p \to r$ 是永真式。若 p 为 1，则 q 和 r 均为 1，即 $q \wedge r$ 和 $q \vee r$ 均为 1，故 $p \to (q \wedge r)$ 和 $p \to (q \vee r)$ 都是永真式。结论成立。

(4) 由条件知，$p \to r$ 和 $q \to r$ 为永真式，即 $\neg p \vee r$ 和 $\neg q \vee r$ 为永真式，从而 $(\neg p \vee r) \wedge (\neg q \vee r)$ 为永真式。又因为

$$(\neg p \vee r) \wedge (\neg q \vee r) \Leftrightarrow (\neg p \wedge \neg q) \vee r \Leftrightarrow (p \vee q) \to r。$$

故 $(p \vee q) \to r$ 为永真式。结论成立。

1.7.2 自然推理系统

严格的论证过程可以采用自然推理系统或公理推理系统实现，这里仅介绍自然推理系统。这种推理的基本思想是，不引入公理，仅依据事先确定的一些推理规则，从前提出发，利用推理规则构造出严格的命题序列，推导出最终的结论。由于这种推理较符合人们的日常思维习惯，故称为“自然推理”，也称为“构造证明法”、“演绎法”或“形式证明”。

1．推理定律

一些重要的逻辑关系如交换律、结合律、德• 摩根律等是基本常识，是构成推理的基础。表 1-5 中列出了最基本的等价关系。

为了完成推理，我们还需要承认一些简单的逻辑关系，以此作为公认的推理规则，而不是所有推理都从零做起。例如，考虑如下的思维（论证）过程：

如果你有口令，那么，你就能登录网络。

你有了口令。

因此，你能登录网络。

如果用 p 表示“你有口令”，q 表示“你能登录网络”，则上述论证过程可描述为：

$$\begin{array}{l} \because\ p \to q \\ \underline{\quad p \quad} \\ \therefore\ q \end{array}$$

这种论证的实质是说，如果有 $p \to q$ 和 p 都为 1 的前提，必有 q 为 1 的结论，故可以用蕴含关系简化描述为：

$$p, p \to q \Rightarrow q,$$

或

$$p \wedge (p \to q) \Rightarrow q。$$

这样的一组基本蕴含关系被确定为可直接应用的推理规则，参见表 1-8。

表 1-8

序号	蕴含关系	含义
I_1 I_2	$p \wedge q \Rightarrow p$ $p \wedge q \Rightarrow q$	化简律
I_3 I_4	$p \Rightarrow p \vee q$ $q \Rightarrow p \vee q$	附加律
I_5 I_6	$\neg p \Rightarrow p \to q$ $q \Rightarrow p \to q$	
I_7 I_8	$\neg(p \to q) \Rightarrow p$ $\neg(p \to q) \Rightarrow \neg q$	
I_9	$p, q \Rightarrow p \wedge q$	
I_{10}	$\neg p, p \vee q \Rightarrow q$	析取三段论
I_{11} I_{12}	$p, p \to q \Rightarrow q$ $\neg q, p \to q \Rightarrow \neg p$	假言推理 拒取式
I_{13}	$p \to q, q \to r \Rightarrow p \to r$	假言三段论
I_{14}	$p \leftrightarrow q, q \leftrightarrow r \Rightarrow p \leftrightarrow r$	等价三段论
I_{15}	$p \vee q, p \to r, q \to r \Rightarrow r$	
I_{16} I_{17}	$p \to q \Rightarrow (p \vee r) \to (q \vee r)$ $p \to q \Rightarrow (p \wedge r) \to (q \wedge r)$	
I_{18} I_{19}	$p \to q, p \to r \Rightarrow p \to (q \vee r)$ $p \to q, p \to r \Rightarrow p \to (q \wedge r)$	

表 1-5 和 1-8 中的 E 和 I 分别表示基本等价和蕴含定律。表中的序号没有意义，但要分清是 I 还是 E。定律的名字能知道更好，真正的要求是理解后记住中间列的蕴含或等价关系，即**推理定律**（也可称蕴含式为**推理规则**(Rules of Inference)，称等价式为**推理定律**（laws））。

简言之，之所以推理定律能用于推理过程，其原因是，若公式 p 为 1，且有 $p \Rightarrow q$ 或 $p \Leftrightarrow q$，那么，一定可以推出 q 为 1。因此，在推理过程中，推理定律可不加证明地引用。

[辨析] 表 1-8 的蕴含关系前提中的逗号（如 I_9）表示两个命题可能在不同的步骤上推得，可能是前提，也可能是中间结论，都是已知的真命题。

[辨析] 表 1-8 所列的基本关系中的肯定形式与否定形式同样有效，如“$\neg p \Rightarrow p \to q$”成立，则“$p \Rightarrow \neg p \to q$”也成立。

2．利用推理定律实现形式证明

形式逻辑推理的本质是说明一个蕴含关系，或者说，总假定前提是真的，再利用表 1-5 和 1-8 所列的基本等价和蕴含关系，说明结论也为真就完成了推理。这种推理就是“因为+所以”组成的步骤，只是每次的“所以”都要由推理定律来保证，且形式上应尽量严格。

为了说明形式推理的过程，这里考虑 1.7.1 节中提及的初等数学问题及证明过程。

① $\because a^2 - b^2 = bc$　　前提

② $\therefore (a^2 - b^2) + b^2 = bc + b^2$　　推理定律：$x = y \Rightarrow x + z = y + z$

③ $\therefore a^2 + (-b^2 + b^2) = b^2 + bc$　　推理定律：$(x + y) + z = x + (y + z)$，$x + y = y + x$

④ $\therefore a^2 + 0 = b(b + c)$　　推理定律：$x + (-x) = 0$，$x(y + z) = xy + xz$

⑤ $\therefore a^2 = b(b + c)$　　推理定律：$x + 0 = x$

⑥ $\because c \neq 0$　　前提

⑦ $\therefore a^2 / c = b(b + c) / c$　　推理定律：$x = y \wedge z \neq 0 \Rightarrow x / z = y / z$。

⑧ $\therefore a^2 / c = b(b / c + 1)$　　推理定律：$(x + y) / z = x / z + y / z$，$x / x = 1$

上述过程与生活中的一般证明过程相同，只是更严格，每得到一个论断都要由公认的定律来保证。右侧的注解说明了推理规则和引用的定律。很明显，如果任何一条推理定律不能得到认可，则推理过程将无法继续。

在推理过程中，前提总认为是真的，而利用推理定律得到的等式就是部分结论，自然也是真的。

命题逻辑的形式推理过程与上述论证过程一致，仅是所涉及的运算（联结词）和定律不同。

例 1-23　证明 $a \to b, \neg(b \vee c) \Rightarrow \neg a$。

证明

① $\because \neg(b \vee c)$ 为 1　　前提引入

② $\therefore \neg b \wedge \neg c$ 为 1　　①德・摩根律

③ $\therefore \neg b$ 为 1　　②化简律

④ $\because a \to b$ 为 1　　前提引入

⑤ $\therefore \neg a$ 为 1　　③④拒取式

此证明过程进一步说明了一个命题由哪些命题推证而来，还可适当简化：

① 推理过程中能够引入的命题公式都应是真的，故“a 为 1”写成“a”就好；

② 除了前提外，所有的中间命题都是“所以”，不必再标记“$\because$”和“$\therefore$”；

③ 推理定律名可不记忆，只要标记出采用等价关系还是蕴含关系（推理定律）即可。

于是，可重新写出证明过程如下：

证明

① $\neg(b\vee c)$	前提引入
② $\neg\, b\wedge\neg\, c$	推理定律，① E
③ $\neg\, b$	推理定律，② I
④ $a\to b$	前提引入
⑤ $\neg\, a$	推理定律，③⑤ I

其中的 E 和 I 分别表示等价和蕴含规则。

很明显，上述推理中仅包含两类引入真命题的形式，可以概括为以下 2 条推理规则：

(1) P **规则**。前提引入规则，指在证明的任何步骤都可引入前提；

(2) T **规则**。推理定律引用规则，指在证明过程中，如一个或几个公式满足推理定律，则其结论或等价公式可引入。

利用 P 规则和 T 规则实现的证明方法称为“直接证明法”。

[辨析] P 和 T 分别是前提（premise）和重言、蕴含（tautology）的意思。

利用直接证法重新写出的证明过程由序号、真命题和理由 3 列组成（下述证明过程中最后添加的列用于解释，实际证明时是不需要的）：

证明

① $\neg(b\vee c)$	P	前提为真
② $\neg\, b\wedge\neg\, c$	T① E	由前提①利用等价关系得到的命题为真
③ $\neg\, b$	T② I	由结论②利用蕴含关系得到的命题为真
④ $a\to b$	P	前提为真
⑤ $\neg\, a$	T③④ I	由结论③和前提④利用蕴含关系得到的命题为真

这样一来，推理形式变得简单且严格。

[辨析] 一个非常重要的事实是这里我们仅承认推理定律，没有置换规则，即不允许子公式替代。例如，由 $p\to(q\to r)$ 的前提不能推出 $p\to(\neg\, q\vee r)$，尽管二者是等价的。除非将子公式替代也定义为一条允许的置换规则。

3．直接证法的形式推理示例

例 1-24　证明 $(p\vee q)\wedge(p\to r)\wedge(q\to s)\Rightarrow s\vee r$。

证明

① $p\vee q$	P
② $\neg\, p\to q$	T① E

③ $q \to s$ P

④ $\neg p \to s$ T②③ I

⑤ $\neg s \to p$ T④ E

⑥ $p \to r$ P

⑦ $\neg s \to r$ T⑤⑥ I

⑧ $s \vee r$ T⑦ E

一种存在问题的证明过程如下：

证明

① $p \to r$ P

② $(p \vee q) \to (r \vee q)$ T① I

③ $q \to s$ P

④ $(q \vee r) \to (s \vee r)$ T③ I

⑤ $(p \vee q) \to (s \vee r)$ T②④ I

⑥ $p \vee q$ P

⑦ $s \vee r$ T⑤⑥ I

此证明过程中存在的错误是，没有直接的蕴含或等价定律保证由步骤②、④推出⑤。要想推出⑤，必须允许置换规则，得到：

⑤' $(p \vee q) \to (q \vee r)$ 置换规则② I

再重写步骤⑤：

⑤ $(p \vee q) \to (s \vee r)$ T④⑤' I

可见，究竟允许哪些推理规则对证明过程影响很大，学习时应注意书中的要求。

例 1-25 证明 $(p \vee q) \to v, v \to (r \vee s), s \to u, \neg r \wedge \neg u \Rightarrow \neg p$。

证明

① $\neg r \wedge \neg u$ P

② $\neg u$ T① I

③ $s \to u$ P

④ $\neg s$ T②③ I

⑤ $\neg r$ T① I

⑥ $\neg r \wedge \neg s$ T④⑤ I

⑦ $\neg(r \vee s)$ T⑥ E

⑧ $v \to (r \vee s)$ P

⑨ $\neg v$ T⑦⑧ I

⑩ $(p \vee q) \to v$ P

⑪ $\neg(p \vee q)$ T⑨,⑩ I

⑫ $\neg p \wedge \neg q$ T⑪ E

⑬ $\neg p$ T⑫ I

4．间接证法

一些题目仅依靠直接证法比较困难，这里引入 2 个新的推理规则作为间接证法。

(3) **不相容规则**。结论的否定可以作为附加前提引入，其结果与前提将是不相容的。

不相容规则就是反证法（或称归谬法）：若证明 $A \Rightarrow C$，可以假定结论 C 不真，即 $\neg C$ 为真，就一定会推出矛盾，也就是得到一个永假式（矛盾式）。这里的“$\neg C$”是作为一个附加前提（不是原始前提）引入的。

例 1-26　证明 $p \to q$，$\neg(q \vee r) \Rightarrow \neg p$。

证明

① $p \to q$	P
② p	P（附加前提）
③ q	T①② I
④ $\neg(q \vee r)$	P
⑤ $\neg q \wedge \neg r$	T③ E
⑥ $\neg q$	T④ I
⑦ $q \wedge \neg q$（矛盾）	T③⑥ I

步骤②就是采用反证法所引入的附加前提。当然，也可以用 $\neg\neg p$ 作为附加前提，只是需要多用一次双重否定律。步骤⑦推出不相容的命题，即一个矛盾式，这就说明了“假定结论不真”是错的。

例 1-27　证明 $(p \vee q) \to (r \wedge s)$，$(s \vee u) \to v \Rightarrow \neg p \vee v$。

证明

① $\neg(\neg p \vee v)$	P（附加前提）
② $\neg\neg p \wedge \neg v$	T① E
③ $\neg\neg p$	T② I
④ p	T③ E
⑤ $p \vee q$	T④ I
⑥ $(p \vee q) \to (r \wedge s)$	P
⑦ $r \wedge s$	T⑤⑥ I
⑧ s	T⑦ I
⑨ $s \vee u$	T⑧ I
⑩ $(s \vee u) \to v$	P
⑪ v	T⑨⑩ I
⑫ $\neg v$	T② I
⑬ $v \wedge \neg v$（矛盾）	T⑪⑫ I

(4) CP（Conditional Proof）**规则**。若证明 $A \Rightarrow B \to C$，B 可作为附加前提引入。

沿用一般的说法，A 为大前提，B 为小前提（即含在结论中的前提），那么，小前提可以与大

前提同样使用。这里的原因是：

$$A \to (B \to C) \Leftrightarrow \neg A \vee (\neg B \vee C) \Leftrightarrow \neg(A \wedge B) \vee C \Leftrightarrow (A \wedge B) \to C。$$

可见，证明 $A \Rightarrow B \to C$ 等同于证明 $A \wedge B \Rightarrow C$，故小前提 B 等同于大前提。

[辨析] CP 规则只应用于结论为条件式的特殊问题，也称为“条件规则”或“条件证明”。

例 1-28 证明 $p \to (q \to u), \neg v \vee p, q \Rightarrow v \to u$。

证明

① v	P（附加前提）
② $\neg v \vee p$	P
③ p	T①② I
④ $p \to (q \to u)$	P
⑤ $q \to u$	T③④ I
⑥ q	P
⑦ u	T⑤⑥ I
⑧ $v \to u$	CP

因为结论为条件式，步骤①引入了小前提 v 作为附加前提，推导出结论 u。步骤⑧只是重写了一遍真实的结论以说明采用了 CP 规则。

[辨析] 何时采用间接证法？观察结论，如果论证呈现如下形式：

(a) $A \Rightarrow C$。结论是单个命题，可用反证法，引入条件为 $\neg C$；

(b) $A \Rightarrow B \vee C$。结论为析取式，可用反证法，引入条件为 $\neg(B \vee C)$，可推出结论 $\neg B$ 和 $\neg C$；

(c) $A \Rightarrow B \to C$。结论为条件式，可用反证法或 CP 规则。若用反证法，引入条件为 $\neg(B \to C)$，可推出结论 B 和 $\neg C$；若用 CP 规则，引入条件 B。

特别地，如果结论是 $A \to B \to C$，可以逐次用 CP 规则，先引入 A，再引入 B。也可以用反证法。

例 1-29 如果雷军努力学习，他就会取得好成绩。若雷军贪玩或不按时写作业，他就不能取得好成绩。所以，如果雷军努力学习，他一定不贪玩且按时完成作业。

解 记 p：雷军努力学习，q：雷军取得好成绩，r：雷军贪玩，s：雷军按时完成作业。则论证要求可符号化为：

$$p \to q, (r \vee \neg s) \to \neg q \Rightarrow p \to (\neg r \wedge s)。$$

证明过程如下：

① p	P（附加前提）
② $p \to q$	P
③ q	T①② I
④ $(r \vee \neg s) \to \neg q$	P
⑤ $\neg(r \vee \neg s)$	T③④ I
⑥ $\neg r \wedge s$	T⑤ E

⑦ $p \to (\neg r \wedge s)$　　CP

由步骤⑤直接得到结论 $\neg r \wedge s$ 而不是 $\neg r \wedge \neg\neg s$，后者在不允许置换规则时还需要展开：

⑥ $\neg r \wedge \neg\neg s$　　T⑤ E

⑦ $\neg r$　　T⑥ I

⑧ $\neg\neg s$　　T⑥ I

⑨ s　　T⑧ E

⑩ $\neg r \wedge s$　　T⑦⑨ I

可见，直接采用否定形式是重要的，既可以简化推理过程，也可以在一定程度上消除子公式替代。

[延伸] 命题逻辑在案件审理、有限情况判定、排队论和电路设计等许多方面具有广泛的应用。不过，应注意不同书籍在自然推理系统中采用的规则、名词存在着一定差异[4-5,9,13-15]。

思考与练习 1.7

1-43　条件式 $p \to q$ 的逆换式、反换式和逆反式各是什么？

1-44　用不构造真值表的非形式方法证明下述推理。

(a) $p \to q \Rightarrow p \to (p \wedge q)$。　　(b) $p \to \neg q$，$\neg r \to p$，$q \Rightarrow r$。

(c) $p \Rightarrow \neg p \to q$。

(d) $(p \wedge q) \to s$，$\neg r$，$\neg s \vee r \Rightarrow \neg p \vee \neg q$。

1-45　验证下述推理是否正确。

(a) 若一个数为实数，则它是复数。若一个数为虚数，则它也是复数。一个数既不是实数，又不是虚数，所以它不是复数。

(b) 若一个数为复数，仅当它是实数或虚数。一个数既不是实数，又不是虚数，所以它不是复数。

1-46　自然推理系统中的 T 规则的含义是什么？为什么此规则是有效的呢？

1-47　用自然推理系统证明下述推理。

(a) $\neg(p \wedge \neg q)$，$\neg q \vee r$，$\neg r \Rightarrow \neg p$。　　(b) $p \to (q \vee r), (s \vee t) \to p, s \vee t \Rightarrow q \vee r$。

(c) $p \wedge q$，$(p \leftrightarrow q) \to (r \vee s) \Rightarrow s \vee r$。　　(d) $p \to q, (\neg q \vee r) \wedge \neg r, \neg(\neg p \wedge s) \Rightarrow \neg s$。

(e) $\neg p \vee q$，$r \to \neg q \Rightarrow p \to \neg r$。　　(f) $p \to \neg q, p \vee r$，$\neg r, \neg s \leftrightarrow q \Rightarrow s$。

(g) $p \to q, (q \wedge \neg r) \to s \Rightarrow (\neg r \wedge \neg s) \to \neg p$。

1-48　用自然推理系统证明论证的有效性：如果小红和小兰去上自习，则小龙也去。已知小芳不去上自习或小红去上自习，且小兰和小芳已经去上自习了，所以小龙也去上自习了。

第 2 章 谓 词 逻 辑

命题逻辑主要研究命题及其演算方法，将原子命题作为基本单位而不再分解。但原子命题没有反映命题内部的逻辑结构，是一种比较“粗糙”的逻辑，一些常见的简单论断也不能用命题逻辑进行推证。例如，著名的苏格拉底三段论：

所有人都是要死的，苏格拉底是人，所以苏格拉底是要死的。

类似地还有亚里士多德三段论：

所有人都是必死的，希腊人都是人，所以希腊人都是必死的。

很明显，上述论断的各命题中包含着重复的概念和性质，如人、苏格拉底、要死的等，而命题逻辑不能反映出这些内涵，仅可符号化为：

$$p \wedge q \Rightarrow r。$$

对于任意的命题 p、q 和 r，这是荒谬的，不可证明的。

建立谓词逻辑的目的是将原子命题进一步拆分成个体词、谓词和量词等非命题成分，研究这些内部成分的逻辑关系和规律。或者说，谓词逻辑将命题逻辑作为子系统，集中研究由非命题成分组成的命题形式和量词的逻辑性质与规律。本章只讨论包含个体谓词和个体量词的谓词逻辑，称为**一阶谓词逻辑**，简称**一阶逻辑**，又称为**狭义谓词逻辑**。

第一个完整谓词逻辑系统是德国逻辑学家 G.弗雷格（Gottlob Frege）在 1879 年建立的。

2.1 谓词、个体词与量词

2.1.1 个体词与谓词

一个简单命题通常是对思维对象（即客体）的属性或多个对象之间的关系进行的判定。谓词逻辑将简单命题细分为两部分，即个体词与谓词，并对个体词的数量进行区分。因此，核心概念包括个体词、谓词及量词。

1．个体词

[定义 2-1] 判断中可以独立存在的具体或抽象的对象，或者说客体称为**个体词**（individual）。

个体词是思维中要考虑的对象，如人、苏格拉底、3、x、思想和意识等。在一个命题中，个体词可能参与如下两类判断：

(1) 只有一个个体词时，命题刻画的是个体词的性质，如：

(a) 花是红的。

(b) $\sqrt{2}$ 是无理数。

(c) 这台连接到本校的电脑运行正常。

(d) 哥白尼指出地球绕太阳转。

这些命题中的个体词包括具体的物、人和一件事，如花、$\sqrt{2}$、这台连接到本校的电脑和哥白尼。当然，也可以是抽象的概念。

(2) 含有 2 个以上的个体词时，命题刻画的是个体词之间的关系，如：

(a) 孙建中比李晓光个子高。

(b) 兔子比乌龟跑得快。

(c) 5 介于 2 和 8 之间。

这些命题中分别有 2 个和 3 个个体词，包括孙建中和李晓光、兔子和乌龟、5 和 2 及 8。

通常，用小写字母表示个体词。一个代表固定个体的符号称为**个体常量**，没有固定指代的个体符号称为**个体变元**。

个体词的取值范围称为**个体域**（domain of individual）或**论域**（universe），用 $\mathscr{D}$ 表示（Domain 的意思），一般是一个集合。例如，对于命题“所有有理数都是实数”可令论域 $\mathscr{D}$ 为实数集，当讨论学生的成绩好坏时可令论域 $\mathscr{D}$ 为全体学生组成的集合。

在没有指明个体域时，表示个体域是由世间万物所组成的集合，称为**全总个体域**，简称**全体域**或**全域**。

2．谓词

[定义 2-2] 判断中描述个体词的性质或相互关系的词称为**谓词**（predicate）。

简单讲，原子命题中除去个体词和数量词之外的部分就是谓词。可见，个体词和谓词基本就是一个句子的主语和谓语。例如，“是红的”、“比……个子高”都是谓词。不过，因为缺少思维的对象，需要在谓词上添加个体变元才能使含义表示完整，如“x 是红的”和“x 比 y 个子高”等，这里的 x、y 表示个体变元。

谓词一般用大写字母（或词）表示，其中用泛指的个体变元表示思维对象，如：

(a) $R(x)$：x 是红的。　　(b) $I(x)$：x 是无理数。

(c) $H(x)$：x 运行正常。　　(d) $P(x)$：x 指出地球绕太阳转。

(e) $T(x,y)$：x 比 y 个高。　　(f) $F(x,y)$：x 比 y 跑得快。

(g) $Between(z,x,y)$：z 介于 x 和 y 之间。

将个体变元用固定个体代替就可表示出前述的简单命题，如 P(哥白尼)、F(兔子, 乌龟)等。

[辨析] 如果引入谓词 $P(x,y)$：x 指出 y，则“哥白尼指出地球绕太阳转”也可以描述为：

$$P(\text{哥白尼, 地球绕太阳转})。$$

上述讨论中的所有谓词如 $R(x)$、$F(x,y)$ 等都具有数学函数形式，故也称为“命题函数”或“简单命题函数”，其中的“R：是红的”和“F：比……跑的快”才是谓词，基本等同于谓语，x 和 y 为个体变元。为了简单，我们仍直接称 $R(x)$、$F(x,y)$ 为谓词。因此，谓词与命题函数是相同的含义，都代表着一个包含 n 个个体变元的谓词，如 $A(x_1,x_2,\cdots,x_n)$。

谓词中个体变元的数量称为谓词的**元数**，故 $A(x_1,x_2,\cdots,x_n)$ 为 n 元谓词，$R(x)$、$F(x,y)$ 和

$Between(z,x,y)$ 分别是一元、二元和三元谓词。这些谓词都有固定的指代，称为**谓词常项**。如果只说明符号 $A(x_1,x_2,\cdots,x_n)$ 是一个 n 元谓词则称其为**谓词变项**。

3．用特殊个体词构成谓词填式

谓词是命题吗？一般不是。一个 n 元谓词中含有 n 个个体词变元，无法确定其值，这如同函数一般不代表一个值一样。

[定义 2-3] 在谓词中将个体词变元用固定的个体词部分或全部代替得到的谓词称为**谓词填式**。这种做法就是将个体词特殊化。

例如，R(花)、F(兔子, y)、$Between$(5, x, y)、$Between$(5, 2, y)、$Between$(5, 2, 8)都是谓词填式。但是，R(花)和 $Between$(5, 2, 8)中已不存在个体词变元，称为 **0 元谓词**。此时，它们已转化为命题。其他谓词仍含有个体词变元，还不是命题。

又如，谓词 $P(x)$表示 $x^2 > x$，论域为实数集合。那么，$P(x)$不是命题，但谓词填式 $P(2)$和 $P(1)$分别表示命题“4>2”和“1>1”，其真值为 1 和 0。

[辨析] 将一个谓词的个体词变元固定为具体的个体词使之成为 0 元谓词就转化为命题。换言之，构造 0 元谓词填式就是指定一个命题函数的“自变量”，使其成为一个固定的命题（值）。

2.1.2 量词与量化

为了使谓词成为命题，可以采取两种办法，分别是对个体词的特殊化和对个体词进行数量限制。特殊化个体词就是前文讨论的谓词填式，而用量词对个体词进行量化可以包括全部和部分两类。

例如，令 $M(x)$表示 x 取得了优异的学习成绩。通过下述方法可将 $M(x)$转化为命题：

(1) 限制个体词数量为全部，如：所有学生取得了优异的学习成绩。

(2) 限制个体词数量仅为部分，如：有的学生取得了优异的学习成绩。

在谓词逻辑中一般只引入两个表示数量的词，称为数量词，一般简称为**量词**（quantifier）。

1．全称量词（universal quantifier）

[定义 2-4] 全称量词符 $\forall$，含义是“所有的”、“全部的”、“任意一个”、“每一个”、“凡是”、“都”、“一切的”（for all，for every，for each，for any，for arbitrary）。$\forall x$ 称为**全称量词**，称 x 为量词（符）$\forall$ 的**指导变元**或**作用变元**。

例 2-1 用符号表示下述命题：

(1) 所有人都是要呼吸的。

(2) 每个学生都要参加考试。

(3) 任何非零整数或是正的或是负的。

解 设 $M(x)$：x 是人，$B(x)$：x 是要呼吸的；

$S(x)$：x 是学生，$T(x)$：x 要参加考试；

$I(x)$：x 是非零整数，$P(x)$：x 是正数，$N(x)$：x 是负数。

那么，上述命题可表示为：

(1) $\forall x(M(x) \to B(x))$；

(2) $\forall x(S(x) \to T(x))$；

(3) $\forall x(I(x) \to (P(x) \triangledown N(x)))$。

2．存在量词（existential quantifier）

[定义 2-5] 存在量词符∃，含义是“存在一些”、“至少有一个”、“有的”（for some，for at least one，there is，there exists）。$\exists x$ 称为**存在量词**，称 x 为量词（符）∃的**指导变元**或**作用变元**。

例 2-2 用符号表示下述命题：

(1) 存在一个数是质数，论域为数的集合。

(2) 有的人聪明。

(3) 有些邮件含有木马。

解 设 $P(x)$：x 是质数；

$M(x)$：x 是人，$C(x)$：x 是聪明的；

$E(x)$：x 是邮件，$H(x)$：x 含有木马。

则命题可表示为：

(1) $\exists x P(x)$；

(2) $\exists x(M(x) \wedge C(x))$；

(3) $\exists x(E(x) \wedge H(x))$。

[辨析] 符号化结果与论域有关。例如，如果论域是人的集合，则(2)可写成$\exists x C(x)$。因为上述命题中没有特殊说明，故论域为全总个体域。

[辨析] 全称量词使用联结词“→”，存在量词使用联结词“∧”，不能互换。此外，量词符∀和∃分别代表着 All 和 Exist 的首字母，只是书写时换了个方向。

由联结词、量词与简单命题函数组成的表达式称为**谓词公式**或**复合命题函数**。事实上，谓词公式可以仿照命题公式来定义，只是要增加对量词∀和∃的描述，即需要肯定 $\forall x P(x)$ 和 $\exists x P(x)$ 都是谓词公式。

思考与练习 2.1

2-1　个体域（论域）、全总个体域的含义是什么？

2-2　在谓词逻辑中，数量词“有一个”，“有一些”和“仅有一个”是一样的含义吗？

2-3　找出下述命题中的个体常量、谓词和量词，并用符号表示出来。

(a) 科比是 NBA 球星。　　(b) $\sqrt{3}$ 是无理数。

(c) 猫喜欢吃鱼。　　(d) 所有有理数都是实数。

(e) 有的人聪明。　　(f) 并非所有人都聪明。

2-4　谓词是命题吗？什么样的谓词是命题？

2-5　你注意到了全称量词 $\forall x$ 和存在量词 $\exists x$ 在表示命题时使用的联结词不同吗？想想为什么。

2.2 谓词逻辑中的命题翻译

由于谓词有谓词填式和量词量化两种转换为命题的方法，实际中也有两类命题需要翻译。

2.2.1 特殊化个体词的命题

当命题中的个体词是固定对象时，不需要关心个体域，只要刻画出表示个体词的性质或个体词之间关系的谓词，并构成谓词填式即可。

例 2-3 用谓词逻辑符号化下述命题：

(1) 苏格拉底是人。

(2) 孙建中比李晓光个子高。

(3) 5 介于 2 和 8 之间。

(4) 若 m 是正数，则 $-m$ 是负数。

(5) 这只大红书柜摆满了那些古书。

解 记 $M(x)$：x 是人；

$T(x, y)$：x 比 y 个子高；

$Between(z, x, y)$：z 介于 x 和 y 之间；

$P(x)$：x 是正数，$N(x)$：x 是负数；

$F(x,y)$：x 摆满了 y。

上述命题可符号化为：

(1) M(苏格拉底)。

(2) T(孙建中, 李晓光)。

(3) $Between(5, 2, 8)$。

(4) $P(m) \to N(-m)$。

(5) F(这只大红书柜, 那些古书)。

如果都表示成符号会更好一些。例如，记 s：苏格拉底，y：孙建中，x：李晓光，a：这只大红书柜，b：那些古书，则(1)、(2)和(5)可用纯符号形式表示为：

(1) $M(s)$。

(2) $T(y, x)$。

(5) $F(a, b)$。

这里对(5)的刻画不够细致。如果将“这只”和“那些”作为个体词，可引入如下谓词：

$R(x)$：x 是大红书柜，$Q(y)$：y 是古书。于是，命题可符号化为如下的谓词填式：

$$R(\text{这只}) \wedge Q(\text{那些}) \wedge F(\text{这只, 那些})。$$

还可以进一步分解那些修饰限定词，即引入如下谓词和个体词符号：

$A(x)$：x 是书柜，$E(y)$：y 是图书，$B(x)$：x 是大的，$C(x)$：x 是红的，$D(y)$：y 是古老的；a：这只，b：那些，则原命题可表示为：

$$A(a) \wedge B(a) \wedge C(a) \wedge E(b) \wedge D(b) \wedge F(a,b)。$$

可见，谓词公式的翻译结果因对个体词性质的刻画程度不同而异。

2.2.2 量词量化的命题

在个体词为泛指时，符号化命题不仅要给出用于刻画表示个体词的性质或个体词之间关系的

谓词（称为“**中心谓词**”），还需要增加一些谓词来描述个体词的范围，这样的谓词称为“**特性谓词**”或“**限定谓词**”。特性谓词的作用是将个体变元局限在满足该谓词代表的性质范围内。如果采用全总个体域，则一定需要这种特性谓词。

一般地，谓词逻辑中的简单命题具有如下形式：

(a) 所有 A 都是 B；　　(b) 存在 A 是 B。

首先，用 $B(x)$表示“x 是 B”，刻画出个体词 x 的性质。但由于个体域为全总个体域，还需要引入特性谓词 $A(x)$表示“x 是 A”，以限定个体变元 x 的取值范围。于是，命题符号化为：

(a) $\forall x(A(x) \to B(x))$；　　(b) $\exists x(A(x) \wedge B(x))$。

例如，对于命题“所有有理数都是实数”，应按如下方式进行符号化：

(1) 引入描述个体词性质的中心谓词 $R(x)$表示：x 是实数。

(2) 引入特性谓词 $Q(x)$表示：x 是有理数。则命题表示为：

$$\forall x(Q(x) \to R(x))。$$

一旦论域局限于特定的范围，特性谓词便不再出现。例如，假定论域 $\mathbb{Q}$ 为有理数集合，则命题可表示为：

$$\forall x R(x)。$$

因为此时所有的个体变元 x 都是有理数。

例 2-4　用谓词逻辑符号化下述命题：

(1) 并非每个实数都是有理数。　　(2) 没有不犯错误的人。

(3) 尽管有人聪明，但未必所有人都聪明。　(4) 所有人都长着黑头发。

(5) 在美国留学的学生未必都是亚洲人。　(6) 骑白马的并不都是王子。

(7) 所有人都不一样高。　　(8) 没有一个自然数大于或等于所有自然数。

解　(1) 记 $R(x)$：x 是实数，$Q(x)$：x 是有理数。符号化为：

$$\neg\ \forall x(R(x) \to Q(x))。$$

(2) 记 $M(x)$：x 是人，$E(x)$：x 犯错误。符号化为：

$$\neg\ \exists x(M(x) \wedge \neg\ E(x))。$$

(3) 记 $M(x)$：x 是人，$C(x)$：x 聪明。符号化为：

$$\exists x(M(x) \wedge C(x)) \wedge \neg\ \forall x(M(x) \to C(x))。$$

(4) 记 $M(x)$：x 是人，$B(x)$：x 长着黑头发。符号化为：

$$\forall x(M(x) \to B(x))。$$

(5) 记 $S(x)$：x 是学生，$A(x)$：x 是在美国留学的，$G(x)$：x 是亚洲人。符号化为：

$$\neg\ \forall x((A(x) \wedge S(x)) \to G(x))。$$

(6) 记 $M(x)$：x 是骑白马的人，$P(x)$：x 是王子。符号化为：

$$\neg\ \forall x(M(x) \to P(x))。$$

(7) 记 $M(x)$：x 是人，$E(x,y)$：x 与 y 相同，$T(x,y)$：x 与 y 一样高。符号化为：

$$\forall x\forall y((M(x)\wedge M(y)\wedge \neg E(x,y))\rightarrow \neg T(x,y))。$$

含义是“对于任意的两个不同的人，他们都不一样高”。

(8) 记 $N(x)$：x 是自然数，$G(x,y)$：$x\geqslant y$。符号化为：

$$\neg \exists x(N(x)\wedge \forall y(N(y)\rightarrow G(x,y)))。$$

例 2-5* 用谓词逻辑符号化下列命题：

(1) 兔子比乌龟跑得快。

(2) 有的兔子比所有的乌龟跑得快。

(3) 并不是所有的兔子都比乌龟跑得快。

(4) 不存在跑得同样快的两只兔子。

解 记特性谓词 $R(x)$：x 是兔子，$G(y)$：y 是乌龟，刻画关系的中心谓词 $F(x,y)$：x 比 y 跑得快，$E(x,y)$：x 与 y 跑得一样快。上述命题可理解并表示为：

(1) 所有的兔子比所有的乌龟跑得快。

$$\forall x\forall y((R(x)\wedge G(y))\rightarrow F(x,y))。$$

(2) 存在一些兔子，它比所有的乌龟跑得快。

$$\exists x(R(x)\wedge \forall y(G(y)\rightarrow F(x,y)))。$$

(3) 并不是所有的兔子都比所有的乌龟跑得快。

$$\neg \forall x\forall y((R(x)\wedge G(y))\rightarrow F(x,y))。$$

(4) $\neg \exists x\exists y(R(x)\wedge R(y)\wedge E(x,y))$。

例 2-6* 用谓词逻辑符号化下列命题：

(1) 不管白猫黑猫，抓住老鼠就是好猫。

(2) 有唯一的偶素数。

(3) 数学分析中极限 $\lim\limits_{x\to a} f(x)=b$ 的定义：任给小的正数 ε，都存在一个正数 δ，使得当 $0<|x-a|<\delta$ 时，有 $|f(x)-b|<\varepsilon$。

(4) 对于每两个点有且仅有一条直线通过该两点。

解 (1) 在不使用二元谓词时可以这样符号化：

记 $C(x)$：x 是抓老鼠的猫，$W(x)$：x 是白的，$B(x)$：x 是黑的，$OK(x)$：x 是好的。命题可表示为：

$$\forall x((C(x)\wedge (W(x)\vee B(x)))\rightarrow OK(x))。$$

以下是使用二元谓词的符号化：

记 $C(x)$：x 是猫，$W(x)$：x 是白的，$B(x)$：x 是黑的，$M(y)$：y 是老鼠，$G(x,y)$：x 抓住 y，$OK(x)$：x 是好的。命题可表示为：

$$\forall x\forall y((C(x)\wedge (W(x)\vee B(x))\wedge M(y)\wedge G(x,y))\rightarrow OK(x))。$$

(2) 记 $E(x)$：x 是偶数，$P(x)$：x 是素数，$Q(x,y)$：$x=y$。命题可表示为：

$$\exists x((E(x)\wedge P(x))\wedge \forall y((E(y)\wedge P(y))\rightarrow Q(x,y)))。$$

[辨析] 量词∃仅表示“有”，“有且仅有一个”可理解为“其他满足相同条件的个体词都与当

前个体词相等”或“不存在其他满足相同条件但与当前个体词不相等的个体词”。例如，(2)可以理解为：存在偶素数，且所有偶素数都与此偶素数相等。

(3) 命题最后的结论是$|f(x)-b|<\varepsilon$，前面的叙述都是条件。可符号化为：

$$\forall\varepsilon(\varepsilon>0\rightarrow\exists\delta(\delta>0\wedge\forall x(0<|x-a|<\delta\rightarrow|f(x)-b|<\varepsilon)))。$$

也可以将其中的量词作用到公式之前：

$$\forall\varepsilon\exists\delta\forall x(\varepsilon>0\rightarrow(\delta>0\wedge(0<|x-a|<\delta\rightarrow|f(x)-b|<\varepsilon)))。$$

(4) 记 $P(x)$：x 是点，$L(y)$：y 是直线，$T(z,x,y)$：z 通过 x 和 y，$Q(x,y)$：x 和 y 相同。可符号化为：

$$\forall x\forall y(((P(x)\wedge P(y)\wedge\neg\ Q(x,y))\rightarrow\exists z((L(z)\wedge T(z,x,y))\wedge\forall w((L(w)\wedge T(w,x,y))\rightarrow Q(z,w)))。$$

对此命题的理解是：对于任意两个不同的点，有一条直线通过，且所有通过这两点的直线都与此直线相同。

[延伸] 存在且唯一一般利用“∃”和“=”来刻画，但也可以引入一个特殊的量词∃!来表示存在且唯一。另外，谓词逻辑在人工智能的知识表示中具有非常重要的应用[17]。

例 2-7* 假设在一个房间里，有一个机器人 robot，一个积木块 box，两个桌子 a、b 和一把椅子 c。开始时，机器人 robot 在椅子 c 附近，且两手是空的，桌子 a 上放着积木块 box，桌子 b 上是空的。机器人将从椅子 c 附近出发，把积木块 box 从桌子 a 上转移到桌子 b 上并返回到原处。试给出问题的初始状态和目标状态的描述。

解　定义如下谓词：

Table(x)：x 是桌子；

Chair(x)：x 是椅子；

Empty(y)：y 双手是空的；

At(y,z)：y 在 z 附近；

On(w,x)：w 在 x 上。

其中，x 的论域为{a,b,c}，y 的论域为{robot}，z 的论域为{a,b,c}，w 的论域为{box}。

问题的初始状态可描述为：

Table(a) ∧ *Table*(b) ∧ *Chair*(c) ∧ *At*(robot, c) ∧ *Empty*(robot) ∧ *On*(box, a)。

问题的目标状态可描述为：

Table(a) ∧ *Table*(b) ∧ *Chair*(c) ∧ *At*(robot, c) ∧ *Empty*(robot) ∧ *On*(box, b)。

事实上，以上为人工智能系统中利用谓词进行知识表达时的一个基本步骤。

思考与练习 2.2

2-6　有哪几种将谓词转换为命题的方式？

2-7　什么是特性谓词？它的作用是什么？

2-8 选择适当的例子将下述谓词公式描述成汉语。

(a) $p(2)$。 (b) $p(a) \to q(a)$。

(c) $\forall x(p(x) \to q(x))$。 (d) $\exists x(p(x) \wedge q(x))$。

(e) $\neg\ \forall x(\neg\ p(x) \to q(x))$。

2-9 在谓词逻辑中符号化下列命题。

(a) Java 是一种广泛应用于网络编程的语言。 (b) 她是非常聪明和美丽的。

(c) 病毒比木马隐藏得更深。 (d) 邓超不是歌手，是演员。

(e) 这个动态页面是用 JSP 或 PHP 设计的。

2-10 在谓词逻辑中符号化下列命题。

(a) 每个人都有自己的爱好。 (b) 有的运动员是大学生。

(c) 没有不要钱的午餐。 (d) 在沈阳工作的人未必都是沈阳人。

(e) 有的题简单，但并非都是简单题。 (f) 不劳动者不得食。

(g) 只有总经理才配有秘书。 (h) 鸟会飞。

(i) 金子是闪光的，但闪光的未必都是金子。 (j) 有的汽车比某些火车跑得快。

(k) 任何金属都可溶解在某种液体中。 (l) 并非运动员都钦佩教练。

(m) 没有最大的自然数。 (n) 没有长相完全相同的人。

2.3 量词约束与谓词公式的解释

2.3.1 量词对个体词变元的作用

在含有量词的谓词公式中，每个量词都与固定的个体变元有关，这带来了谓词逻辑的复杂性。

[定义 2-6] 量词的作用范围称为量词的**作用域**或**辖域**（scope）。

例 2-8 说明公式$\exists x((E(x) \wedge P(x)) \wedge \forall y((E(y) \wedge P(y)) \to Q(x, y)))$中量词的辖域。

解 量词$\exists x$的辖域是$((E(x) \wedge P(x)) \wedge \forall y((E(y) \wedge P(y)) \to Q(x, y)))$，量词$\forall y$的辖域是$((E(y) \wedge P(y)) \to Q(x, y))$。

[定义 2-7] 在量词$\exists x$或$\forall x$的辖域内出现的一切 x 称为是受此量词约束的变元，即**受约束变元**（bound variable），没有量词约束的个体变元称为**自由变元**（free variable）。

例 2-9 说明公式$\forall y((E(y) \wedge P(y)) \to Q(x, y))$中变元的类型。

解 变元 y 是受量词$\forall y$约束的变元，而 x 是自由变元。

在公式复杂时，变元可能重名，为避免混淆，常常需要对公式进行规范，即将不同变元用不同的名字表示。此时，需要注意的是相同的名字可能代表不同的对象，要仔细分辨，且新引入名字不能与已有名字重复。

例如，对$\forall x(P(x) \to R(x, y)) \wedge Q(x, y)$中的个体词变元进行规范。可以调整约束变元名，称为**换名**：

$$\forall z(P(z) \to R(z,y)) \wedge Q(x,y)。$$

注意公式中同名的 x 并非都代表相同的个体变元。

也可以调整自由变元名，称为**代入**：

$$\forall x(P(x) \to R(x,y)) \wedge Q(z,y)。$$

[辨析] 名字调整不过是使不同的变元名字唯一，很少需要细分什么是换名，或者什么是代入。

从优先级来说，需要注意∀和∃高于所有联结词，即 $\forall xP(x) \to Q(x)$ 等同于 $(\forall xP(x)) \to Q(x)$，而不是 $\forall x(P(x) \to Q(x))$。

2.3.2　谓词公式的解释与求值

命题公式的解释（取值）只涉及原子命题变元的赋值，但谓词公式的解释需要考虑个体域、公式中包含的命题变元和常量、个体变元和常量，尤其是谓词本身。每种成分都需要经过赋值，才能最终确定谓词公式的真值。

[定义 2-8] 若谓词公式 A 的论域为 $\mathscr{D}$，按下述规则指定的一组赋值称为对 A 的一个**解释**（interpretation），记作 I：

(1) 对每个个体常量指定为 $\mathscr{D}$中的一个元素；

(2) 对每个 n 元谓词变项指定一个具体谓词，即一个含有 n 个个体变元且取值为 1 或 0 的函数；

(3) 对每个 m 元函数指定一个具体函数，即一个含有 m 个自变量，且自变量和函数值均取自于 $\mathscr{D}$的函数。

例 2-10　求谓词公式的值：

$$\forall x(p \to Q(f(x))) \vee R(t)。$$

其中，p：3>1，$Q(x)$：$x \leqslant 3$，$R(x)$：$x>5$，$f(x)=x$，$t=5$，论域 $\mathscr{D}=\{-2,3,6\}$。

要对公式进行解释，首先需要确定论域 $\mathscr{D}=\{-2,3,6\}$，才能解释量词∀和个体变元 x 的意义。其次，要指定公式中含有的各种成分：

(1) 个体常量 t 为 5；

(2) 0 元谓词（命题）p 为 3>1，一元谓词 $Q(x)$和 $R(x)$分别为 $x \leqslant 3$ 和 $x>5$；

(3) 一元函数 $f(x)$为 $f(x)=x$，这样的函数代表着将 $\mathscr{D}$中的若干个体转换另一些个体。

最后，为了求得谓词公式的值，还必须解决量词在有限域上的展开（解释）问题。

对于任何一个论域 $\mathscr{D}$及其上的谓词 $P(x)$，全称量词约束的命题 $\forall xP(x)$ 为 1，当且仅当对 $\mathscr{D}$ 中的每个 x，使 $P(x)$都为 1；存在量词约束的命题 $\exists xP(x)$ 为 1，当且仅当 $\mathscr{D}$中存在某个 x，使 $P(x)$为 1。如果论域是有限的，量词可用对个体的枚举取代，即设论域 $\mathscr{D}=\{a_1,a_2,\cdots,a_n\}$，则有

$$\forall xA(x) \Leftrightarrow A(a_1) \wedge A(a_2) \wedge \cdots \wedge A(a_n),$$
$$\exists xA(x) \Leftrightarrow A(a_1) \vee A(a_2) \vee \cdots \vee A(a_n)。$$

为什么会有如此结论？假设论域 $\mathscr{D}=\{1,2,3\}$，现考虑命题“所有元素都大于 2”。

为了验证命题是否为 1，记 $A(x)$：$x>2$，则原命题的符号表示为：

$$\forall xA(x)。$$

很明显，我们需要验证每个命题（谓词填式）$A(1)$、$A(2)$、$A(3)$。只有所有命题都为 1，原命题才为 1，否则为 0，恰好等同于 3 个命题的合取。

存在量词的分析类似。

特别地，如果论域 $\mathscr{D}$ 为空，隐含 $\forall xP(x)$ 为 1 而 $\exists xP(x)$ 为 0。

[理解] 这个有限域上的等价关系非常重要，是分析谓词公式的主要工具。

现在可以对例 2-10 中的谓词公式求值：

解 由 $p=3>1$ 知 p 为 1，$R(t)=R(5)=5>5$ 为 0，将命题在有限域上展开，有

$$\begin{aligned}&\forall x(p\to Q(f(x)))\vee R(t)\\&\Leftrightarrow \forall x(p\to Q(x))\vee R(t)\\&\Leftrightarrow ((1\to Q(-2))\wedge(1\to Q(3))\wedge(1\to Q(6)))\vee 0\\&\Leftrightarrow (1\to 1)\wedge(1\to 1)\wedge(1\to 0)\\&\Leftrightarrow 0。\end{aligned}$$

[定义 2-9] 任何解释下均为 1 的谓词公式称为**永真式**或**有效式**，至少存在一种解释使其为 1 的谓词公式称为**可满足式**，否则称为**永假式**或**不可满足式**。

例如，$\forall xP(x)\to P(t)$ 为永真式。这是因为，若 $\forall xP(x)$ 为 1，则对论域中的所有个体 y，$P(y)$ 为 1。t 是其中一个个体，自然有 $P(t)$为 1。

2.3.3 量词与联结词的搭配

为什么不同量词在符号化时存在联结词的差别，即全称量词用“条件”联结词，而存在量词用“合取”联结词呢？

(1) 全称量词的符号化

记 $Q(x)$：x 是有理数，$R(x)$：x 是实数。考虑命题：有理数都是实数。符号表示为：

$$\forall x(Q(x)\to R(x))。$$

而不是 $\forall x(Q(x)\wedge R(x))$。

由常识可知，此命题是恒真的，与论域无关。现考虑论域 $\mathscr{D}=\{\sqrt{5}\}$，有

$$\forall x(Q(x)\to R(x))\Leftrightarrow Q(\sqrt{5})\to R(\sqrt{5})\Leftrightarrow 0\to ?\Leftrightarrow 1。$$

但是，$\forall x(Q(x)\wedge R(x))\Leftrightarrow Q(\sqrt{5})\wedge R(\sqrt{5})\Leftrightarrow 0\wedge ?\Leftrightarrow 0$。

可见，不能使用后一种方式符号化。

(2) 存在量词的符号化

仍采用前述的谓词记号。考虑命题：有些实数是有理数。符号表示为：

$$\exists x(R(x)\wedge Q(x))。$$

而不是 $\exists x(R(x)\to Q(x))$。

此命题的真假与论域有关。对于论域 $\mathscr{D}=\{2i\}$，此命题应为假，因为论域中唯一的个体是复数 $2i$，不存在是有理数的实数。

$$\exists x(R(x)\wedge Q(x)) \Leftrightarrow R(2i)\wedge Q(2i) \Leftrightarrow 0\wedge 0 \Leftrightarrow 0 。$$

可见，符号化后的命题在有限域上得到的真值是正确的，但采用条件联结词符号化的结果是错误的：

$$\exists x(R(x)\to Q(x)) \Leftrightarrow R(2i)\to Q(2i) \Leftrightarrow 0\to ? \Leftrightarrow 1 。$$

思考与练习 2.3

2-11　指出下述公式中的约束变元和自由变元，并说明量词的辖域。

(a) $\forall x P(x)\to Q(x)$。　(b) $\exists x\forall y(p(x)\wedge q(y))\to\forall x(r(x))$。

(c) $\exists x\forall y(p(x,y)\to r(x))$。　(d) $\exists x(p(x)\wedge\forall y(q(y)\to r(x,y,z)))$。

2-12　举例说明全称量词 $\forall$ 和存在量词 $\exists$ 在符号化命题时使用的联结词的差异。

2-13　一个谓词公式的解释是什么意思？包括哪些部分？

2-14　计算下述公式的真值。

(a) $\forall x F(x)\to\exists y G(y)$，论域 $\mathscr{D}=\{1,2,3\}$，$F(x)$：x 是偶数，$G(x)$：x 是奇数。

(b) $p(2)\vee\forall x(r(x)\to q(x))$，论域 $\mathscr{D}=\{-3,2,4\}$，$p(x)$：$x>2$，$r(x)$：$x\leqslant 2$，$q(x)$：$x<3$。

(c) $\forall x(\exists x p(x)\to q(x))$，论域 $\mathscr{D}=\{a,b,c\}$，$p(a)=1$，$p(b)=1$，$p(c)=0$；$q(a)=0$，$q(b)=1$，$q(c)=0$。

2-15　设论域 $\mathscr{D}=\{1,2\}$，a=1，指定函数 f 和谓词 p、q 如表 2-1。

表 2-1

$f(1)$	$f(2)$	$p(1)$	$p(2)$	$q(1,1)$	$q(1,2)$	$q(2,1)$	$q(2,2)$
2	1	0	1	1	1	0	0

计算下述公式的真值。

(a) $\forall x(p(x)\to q(f(x),a))$。　(b) $\forall x\exists y(p(x)\wedge q(x,y))$。

2.4　谓词逻辑中的基本等价和蕴含关系

众所周知，“没有不犯错误的人”与“所有人都犯错误”是等同的说法。这样的关系还有很多，要从根本上弄清楚它们为什么等同（等价），这也是实现推理的基本要求。

下述定义将等价与蕴含概念从命题逻辑推广到谓词逻辑。

[定义 2-10] 若两个谓词公式 A 和 B 有相同的论域，且在任何解释下 A 与 B 有相同的真值，则称谓词公式 A 与 B **等价**，记作 $A\Leftrightarrow B$ 或 $A\equiv B$。

如果不考虑谓词本身的可变性，此定义基本等同于高等数学中函数相等的定义。

[定义 2-11] 若两个谓词公式 A 和 B 有相同的论域，且在任何解释下 $A\to B$ 为 1，则称谓词公式 A **蕴含** B，记作 $A\Rightarrow B$。

[辨析] 严格地说，谓词公式的永真式、永假式、可满足式、等价及蕴含的概念都与论域有关，换言之，这些定义都是相对于具体论域而言的。只有论域为全总个体域时才能得到真正意义上的永真式、永假式、可满足式，以及等价和蕴含关系。

2.4.1 基本等价与蕴含关系

1. 命题逻辑的推广

一般地，得到谓词公式的等价关系和蕴含关系可以借助命题公式做形式上的推导，例如：

$$\forall x(P(x)\to Q(x))\Leftrightarrow\forall x(\neg P(x)\vee Q(x))。$$

这里的 $P(x)$和 $Q(x)$具有命题形式，是一种纯形式上的等价变换或置换。又如，

$$\forall xP(x)\to\exists xQ(x)\Leftrightarrow\neg\ \forall xP(x)\vee\exists xQ(x)。$$

公式中的 $\forall xP(x)$ 和 $\exists xQ(x)$ 都是命题，可以依据命题逻辑理论进行等价变换。

不过，谓词逻辑本身也存在一些特殊的等价和蕴含关系。

2. 量词的转换

如果否定命题 $\forall x(x>0)$ 会得到什么呢？答案是 $\exists x(x\not>0)$，即 $\exists x(x\leqslant 0)$，否定所有数都是正数等同于至少存在一个非正数。相对地，否定 $\exists x(x>0)$ 就得到了 $\forall x(x\leqslant 0)$，即不存在一个正数等同于都是非正数。

由此可见，全称量词和存在量词可利用¬联结词进行转换：

$$\neg\ \forall xA(x)\Leftrightarrow\exists x\neg\ A(x)，\ \neg\ \exists xA(x)\Leftrightarrow\forall x\neg\ A(x)。$$

上述关系在有限论域上可直接证明。例如，若论域 $\mathscr{D}=\{a_1,a_2,\cdots,a_n\}$，有

$$\begin{aligned}\neg\ \forall x(A(x))&\Leftrightarrow\neg(A(a_1)\wedge A(a_2)\wedge\cdots\wedge A(a_n))\\&\Leftrightarrow\neg\ A(a_1)\vee\neg\ A(a_2)\vee\cdots\vee\neg\ A(a_n)\\&\Leftrightarrow\exists x\neg\ A(x)。\\\neg\ \exists x(A(x))&\Leftrightarrow\neg(A(a_1)\vee A(a_2)\vee\cdots\vee A(a_n))\\&\Leftrightarrow\neg\ A(a_1)\wedge\neg\ A(a_2)\wedge\cdots\wedge\neg\ A(a_n)\\&\Leftrightarrow\forall x\neg\ A(x)。\end{aligned}$$

这种等价性不受论域的影响。例如，容易理解，命题“不是所有学生都通过了考试”等同于“有的学生没通过考试”，即二者逻辑等价。若记 $S(x)$：x 是学生，$P(x)$：x 通过了考试，则可符号化为：

$$\neg\ \forall x(S(x)\to P(x))\Leftrightarrow\exists x(S(x)\wedge\neg\ P(x))\Leftrightarrow\exists x\neg(S(x)\to P(x))。$$

同样，命题“没有不犯错误的人”等价于“所有人都犯错误”。若记 $M(x)$：x 是人，$E(x)$：x 犯错误，则可符号化为：

$$\neg\ \exists x(M(x)\wedge\neg\ E(x))\Leftrightarrow\forall x(M(x)\to E(x))\Leftrightarrow\forall x\neg(M(x)\wedge E(x))。$$

上述转换关系称为“量词转化律”或“量词否定等价式”，在谓词演算中至关重要，它说明：否定全称量词等价于存在量词加上对谓词的否定，否定存在量词等价于全称量词加上对谓词的否定。

基本上，总是可以按有限论域来分析和衡量谓词公式间是否等价。

3．量词作用域的扩张与收缩

若 B 是不包含 x 的命题或谓词公式，很容易说明如下基本等价关系：

$$\forall x(A(x)\vee B)\Leftrightarrow \forall xA(x)\vee B,\quad \forall x(A(x)\wedge B)\Leftrightarrow \forall xA(x)\wedge B。$$

$$\exists x(A(x)\vee B)\Leftrightarrow \exists xA(x)\vee B,\quad \exists x(A(x)\wedge B)\Leftrightarrow \exists xA(x)\wedge B。$$

量词作用域扩张就是增大，作用域收缩就是缩小。因为 $\wedge$、$\vee$ 满足交换律，B 在 $A(x)$的前、后均可。

量词后使用其他联结词如$\rightarrow$、$\leftrightarrow$时也存在这样的等价关系吗？考虑如下示例：

$$\begin{aligned}\forall x(A(x)\rightarrow B)&\Leftrightarrow \forall x(\neg A(x)\vee B)\Leftrightarrow \forall x\neg A(x)\vee B\\&\Leftrightarrow \neg\exists xA(x)\vee B\Leftrightarrow \exists xA(x)\rightarrow B。\\\forall x(B\rightarrow A(x))&\Leftrightarrow \forall x(\neg B\vee A(x))\Leftrightarrow \neg B\vee\forall xA(x)\\&\Leftrightarrow B\rightarrow\forall xA(x)。\end{aligned}$$

这说明，只有在条件式的前件不含有受约束变元时，量词的作用域才能直接扩张或收缩，否则量词会产生变化。

因为存在上述等价关系，容易说明下述两种极限定义的表示方法等价：

$$\forall\varepsilon(\varepsilon>0\rightarrow\exists\delta(\delta>0\wedge\forall x(0<|x-a|<\delta\rightarrow|f(x)-b|<\varepsilon))),$$

$$\forall\varepsilon\exists\delta\forall x(\varepsilon>0\rightarrow(\delta>0\wedge(0<|x-a|<\delta\rightarrow|f(x)-b|<\varepsilon)))。$$

双条件式$\leftrightarrow$可以参照条件式来考虑。

[辨析] 在不能完全肯定含有复杂联结词的等价关系时，可先将其先转换为 $\wedge$、$\vee$ 表示的公式后再试。

应注意命题公式中的 B 并非一定是命题常量，可以是一般谓词，只要与 x 无关即可，如 $B(y)$。

4．量词分配律

全称量词本身是合取之意，存在量词则意味着析取。因此，有

$$\forall x(A(x)\wedge B(x))\Leftrightarrow \forall xA(x)\wedge\forall xB(x),\quad \exists x(A(x)\vee B(x))\Leftrightarrow \exists xA(x)\vee\exists xB(x)。$$

例如，“所有人唱歌且跳舞”等同于“所有人唱歌且所有人跳舞”，“有人唱歌或跳舞”等同于“有人唱歌或有人跳舞”。

5．量词与联结词结合的蕴含式

对量词 $\forall x$ 和 $\exists x$ 有如下 2 个最基本的蕴含关系：

$$\forall xA(x)\vee\forall xB(x)\Rightarrow \forall x(A(x)\vee B(x)),\quad \exists x(A(x)\wedge B(x))\Rightarrow \exists xA(x)\wedge\exists xB(x)。$$

例如，共 10 个人参加一个联欢会。“10 个人都唱歌或 10 个人都跳舞”一定能推出“10 个人都唱歌或跳舞”。反之，“10 个人中 5 个唱歌、5 个跳舞”不能推出“10 个人都唱歌或 10 个人都跳舞”。类似地，“有的学生通过了数学考试和外语考试”能推出“有的学生通过了数学考试且有的学生通过了外语考试”，反之不能。

也可以通过逻辑分析来说明。若 $\forall xA(x)\vee\forall xB(x)$ 为 1，则 $\forall xA(x)$ 为 1 或 $\forall xB(x)$ 为 1。不妨设 $\forall xA(x)$ 为 1，则对论域中的所有 x，有 $A(x)$ 为 1，故 $A(x)\vee B(x)$ 为 1。因此，$\forall x(A(x)\vee B(x))$ 为 1，蕴含关系成立。

[辨析] 上述两个蕴含式互为逆否命题。只要第一个蕴含式成立，其逆否命题自然就成立：

$$\neg\ \forall x(A(x)\vee B(x))\Rightarrow\neg(\forall xA(x)\vee\forall xB(x))。$$

等价变形后就得到了第二个蕴含式：

$$\exists x(\neg\ A(x)\wedge\neg\ B(x))\Rightarrow\exists x\neg\ A(x)\wedge\exists x\neg\ B(x)。$$

6．多量词的等价与蕴含关系*

量化二元及以上的多元谓词时需要使用多个量词，称为“嵌套量词”。为简单，只考虑 2 个量词的情况，共有以下 8 种量化方式：

(a) $\forall x\forall yA(x,y)$、$\forall y\forall xA(x,y)$；　　(b) $\exists x\exists yA(x,y)$、$\exists y\exists xA(x,y)$；

(c) $\forall x\exists yA(x,y)$、$\exists y\forall xA(x,y)$；　　(d) $\forall y\exists xA(x,y)$、$\exists x\forall yA(x,y)$。

容易想象，(a)、(b)两组中的公式是等价的，但(c)、(d)两组中的公式是不等价的。

例如，设论域 $\mathscr{D}=\{0,1\}$，考虑命题 $\forall x\exists y(x+y=0)$ 和 $\exists y\forall x(x+y=0)$，对应的自然语言描述为：

① $\forall x\exists y(x+y=0)$：对所有 x，有 y，使 $x+y=0$。

② $\exists y\forall x(x+y=0)$：存在 y，对所有 x，有 $x+y=0$。

因为

$$\forall x\exists y(x+y=0)\Leftrightarrow\exists y(0+y=0)\wedge\exists y(1+y=0)。$$

且 0+0=0，1+(–1)=0，故命题 $\forall x\exists y\big(x+y=0\big)$ 为 1。但是，不存在一个整数，使其与 0 和 1 的和都为 0，$\exists y\forall x(x+y=0)$ 为 0。

为了理解含有嵌套量词的谓词公式，一般可设论域为 $\mathscr{D}=\{a,b\}$，再将量词在有限域上转换为谓词填式，如：

$$\begin{aligned}\forall x\exists y\,A(x,y)&\Leftrightarrow\exists yA(a,y)\wedge\exists yA(b,y)\\&\Leftrightarrow(A(a,a)\vee A(a,b))\wedge(A(b,a)\vee A(b,b))\\&\Leftrightarrow(p\vee q)\wedge(r\vee s)。\\\exists x\forall y\,A(x,y)&\Leftrightarrow(p\wedge q)\vee(r\wedge s)。\end{aligned}$$

这里的 $p=A(a,a)$，$q=A(a,b)$，$r=A(b,a)$，$s=A(b,b)$。于是，在命题逻辑中就可以推证二者的等价性和蕴含关系。

应注意在将量词转换成谓词填式时的次序不能错，即不同量词的顺序不能交换，要按由外到内的次序展开。

2.4.2　利用等价关系计算前束范式

谓词演算也可以像命题演算那样转换为规范形式，但要利用等价关系扩张量词的作用域，将所有量词都作用到整个公式的开头，即使作用域为整个公式。

[定义 2-12] 一个谓词公式，如果所有量词作用于公式开头，作用域延伸到公式末尾，则称其为**前束范式**或**前缀范式**，形如：

$$\square x_1 \square x_2 \cdots \square x_n A(x_1, x_2, \cdots, x_n)。$$

其中的□表示量词符∀或∃，而谓词公式 $A(x_1, x_2, \cdots, x_n)$不含量词符。

可以证明，任何谓词公式都等价于一个前束范式。先将一个公式中的不同变元唯一化（通过换名或代入使不同的名字互不重复），再通过等价关系将量词作用域扩张到整个公式之前即可实现。因为所有联结词均可以转换为 ¬、∧、∨ 表示，故这样的变换仅涉及到如下几种直接的等价变形：

$$\neg\ \forall x A(x) \Leftrightarrow \exists x \neg\ A(x),$$

$$\neg\ \exists x A(x) \Leftrightarrow \forall x \neg\ A(x),$$

$$\forall x A(x) \wedge \forall x B(x) \Leftrightarrow \forall x (A(x) \wedge B(x)),$$

$$\exists x A(x) \vee \exists x B(x) \Leftrightarrow \exists x (A(x) \vee B(x))。$$

在量词作用域不能直接扩张时，需要采用经过变元换名后的等价关系：

$$\forall x A(x) \vee \forall x B(x) \Leftrightarrow \forall x \forall y (A(x) \vee B(y)),$$

$$\exists x A(x) \wedge \exists x B(x) \Leftrightarrow \exists x \exists y \big(A(x) \wedge B(y)\big)。$$

例 2-11　求公式 $(\neg\ \forall x(p(x)) \vee \exists x(q(x))) \wedge \exists x(s(x))$ 的前束范式。

解　原式 $\Leftrightarrow (\exists x(\neg\ p(x)) \vee \exists x(q(x))) \wedge \exists x(s(x))$　　注：量词转换

$\Leftrightarrow \exists x(\neg\ p(x) \vee q(x)) \wedge \exists x(s(x))$　　注：$\exists x$ 分配律

$\Leftrightarrow \exists x(\neg\ p(x) \vee q(x)) \wedge \exists y(s(y))$　　注：变元换名

$\Leftrightarrow \exists x \exists y((\neg\ p(x) \vee q(x)) \wedge s(y))$ 。　　注：$\exists y$ 扩张

前束范式仍可以进一步转换成析取范式或合取范式，构成前束析取范式和前束合取范式。此例就是前述合取范式。将一个公式转换为前束范式的目的是为了简化对公式内部成分的分析。

[延伸] 可以证明，前束范式中的所有存在量词均可以移至全称量词之前，这样的范式称为“斯科林（Skolem）范式”。斯科林范式可进一步简化对谓词公式的研究，也被用在定理的机器证明方法如“消解法”中[18]。

思考与练习 2.4

2-16　谓词公式 A 与 B 等价的含义是什么？

2-17　$\forall x(A(y) \to B(x))$等价于 $A(y) \to \forall x B(x)$ 吗？$\forall x(A(x) \to B(y))$ 等价于 $\forall x A(x) \to B(y)$ 吗？

2-18　利用有限域说明 $\forall x A(x) \vee \forall x B(x) \Rightarrow \forall x(A(x) \vee B(x))$ 。

2-19　证明 $\exists x(p(x) \to q(y)) \Leftrightarrow \forall x(p(x)) \to q(y)$ 。

2-20　证明 $\forall x(p(x) \wedge q(x)) \Leftrightarrow \forall x(p(x)) \wedge \forall x(q(x))$ 。

2-21 证明 $\neg\exists x(p(x)\wedge q(a))\Rightarrow\forall x(p(x))\rightarrow\neg q(a)$，$a$ 为个体常量。

2-22 指出下述推证中的错误。

$$\forall x(p(x)\rightarrow q(x))\Leftrightarrow\forall x(\neg p(x)\vee q(x))\Leftrightarrow\forall x\neg(p(x)\wedge\neg q(x))$$
$$\Leftrightarrow\neg\exists x(p(x)\wedge\neg q(x))\Leftrightarrow\neg\exists x(p(x))\wedge\exists x(\neg q(x))$$
$$\Leftrightarrow\neg\exists x(p(x))\vee\neg\exists x(\neg q(x))\Leftrightarrow\neg\exists x(p(x))\vee\forall x(q(x))$$
$$\Leftrightarrow\exists x(p(x))\rightarrow\forall x(q(x))。$$

2-23 求下述公式的前束范式。

(a) $\forall x(p(x)\rightarrow\exists yq(x,y))$。 (b) $\exists x(\neg\exists y(p(x,y))\rightarrow(\exists z(q(z))\rightarrow r(x)))$。

2-24 求下述公式的前束合取范式和析取范式。

(a) $(\exists xP(x)\vee\exists xQ(x))\rightarrow\exists x(P(x)\vee Q(x))$。

(b) $\forall x(P(x)\rightarrow\forall y(\forall zQ(z,y)\rightarrow\neg\forall zR(x,y,z)))$。

2.5 谓词演算的推理理论

1．推理定律

谓词演算中也存在一些基本的等价与蕴含关系，参见表 2-2。我们以此作为推理的基础，即推理定律。

表 2-2

序号	等价或蕴含关系	含义
E_{27}	$\neg\forall xA(x)\Leftrightarrow\exists x\neg A(x)$	量词否定等值式
E_{28}	$\neg\exists xA(x)\Leftrightarrow\forall x\neg A(x)$	
E_{29}	$\forall x(A(x)\wedge B(x))\Leftrightarrow\forall xA(x)\wedge\forall xB(x)$	量词分配等值式（量词分配律）
E_{30}	$\exists x(A(x)\vee B(x))\Leftrightarrow\exists xA(x)\vee\exists xB(x)$	
E_{31}	$\forall x(A(x)\vee B)\Leftrightarrow\forall xA(x)\vee B$	量词作用域的扩张与收缩
E_{32}	$\forall x(A(x)\wedge B)\Leftrightarrow\forall xA(x)\wedge B$	
E_{33}	$\exists x(A(x)\vee B)\Leftrightarrow\exists xA(x)\vee B$	
E_{34}	$\exists x(A(x)\wedge B)\Leftrightarrow\exists xA(x)\wedge B$	
E_{35}	$\forall x(B\vee A(x))\Leftrightarrow B\vee\forall xA(x)$	
E_{36}	$\forall x(B\wedge A(x))\Leftrightarrow B\wedge\forall xA(x)$	
E_{37}	$\exists x(B\vee A(x))\Leftrightarrow B\vee\exists xA(x)$	
E_{38}	$\exists x(B\wedge A(x))\Leftrightarrow B\wedge\exists xA(x)$	
E_{39}	$\exists x(A(x)\rightarrow B(x))\Leftrightarrow\forall xA(x)\rightarrow\exists xB(x)$	
E_{40}	$\forall x(A(x)\rightarrow B)\Leftrightarrow\exists xA(x)\rightarrow B$	
E_{41}	$\exists xA(x)\rightarrow B\Leftrightarrow\forall x(A(x)\rightarrow B)$	
E_{42}	$A\rightarrow\forall xB(x)\Leftrightarrow\forall x(A\rightarrow B(x))$	
E_{43}	$A\rightarrow\exists xB(x)\Leftrightarrow\exists x(A\rightarrow B(x))$	
I_{20}	$\forall xA(x)\vee\forall xB(x)\Rightarrow\forall x(A(x)\vee B(x))$	
I_{21}	$\exists x(A(x)\wedge B(x))\Rightarrow\exists xA(x)\wedge\exists xB(x)$	
I_{22}	$\exists xA(x)\rightarrow\forall xB(x)\Rightarrow\forall x(A(x)\rightarrow B(x))$	

表 2-2 中的 I、E 序号是接着表 1-5 和 1-8 排列的，表明它们都是谓词逻辑的推理定律。E_{31}~E_{34} 与 E_{35}~E_{38} 只是 A 和 B 的顺序不同。

2．量词的消除与产生规则

谓词推理可以看作是对命题推理的扩充。除了原来的 P 规则（前提引入）、T 规则（命题等价和蕴含）及反证法、CP 规则外，为什么还需引入新的推理规则呢？

命题逻辑中只有一种命题，但谓词逻辑中有 2 种，即量词量化的命题和谓词填式命题。如果仅由表 2-2 的推理定律就可推证，并不需要引入新的规则，但这种情况十分罕见，也失去了谓词逻辑本身的意义。为此，要引入如下 4 个规则完成量词量化命题与谓词填式之间的转换，其中的 $A(x)$表示任意的谓词。

(1) **全称指定（消去）规则 US**（Ubiquity Specification，或记为∀-）

此规则也可记作 UI（Universal Instantiation），即全称（量词）实例化。

若 $\forall xA(x)$ 为 1，则 $A(a)$ 为 1，即

$$\frac{\because\ \forall xA(x)}{\therefore\ \ A(a)}$$

其中的 a 为论域中的任意一个个体（arbitrary individual），但不能与 A 中的其他个体名重复。

例如，由前提 $\forall x(P(x)\to Q(y))$ 可实例化为 $P(t)\to Q(y)$，而不能是 $P(y)\to Q(y)$。

(2) **全称推广（产生）规则 UG**（Ubiquity Generalization，或记为∀+）

若 $A(a)$ 为 1，则 $\forall xA(x)$ 为 1，即

$$\frac{\because\ A(a)}{\therefore \forall xA(x)}$$

其中的 a 必须是论域中的任意个体，即来自于全称指定规则，但 x 不能与 A 中的其他个体名重复。

在前例中，y 为自由变元，由 $P(t)\to Q(y)$ 可推广为 $\forall x(P(x)\to Q(y))$，但不能是 $\forall y(P(y)\to Q(y))$。

(3) **存在指定（消去）规则 ES**（Existence Specification，或记为∃-）

此规则也可记作 EI（Existence Instantiation），即存在（量词）实例化。

若 $\exists xA(x)$ 为 1，则 $A(s)$ 为 1，即

$$\frac{\because\ \exists xA(x)}{\therefore\ \ A(s)}$$

其中的 s 为论域中的某个特殊个体（some individual），不能与 A 中的其他个体名、前提或结论以及前期推理步骤中的自由个体名重复。

例如，考虑推理 $\exists xP(x)$，$\exists x(P(x)\wedge Q(y))\Rightarrow Q(s)$ 的论证。

① $\exists xP(x)$	P
② $P(u)$	∃-①
③ $\exists x(P(x)\wedge Q(y))$	P
④ $P(v)\wedge Q(y)$	∃-②

在步骤②中用 u 做存在量词实例化，它必须与 y 和 s 都不相同。在步骤④中用 v 做存在量词实例化，它必须与 u、y 和 s 都不相同。

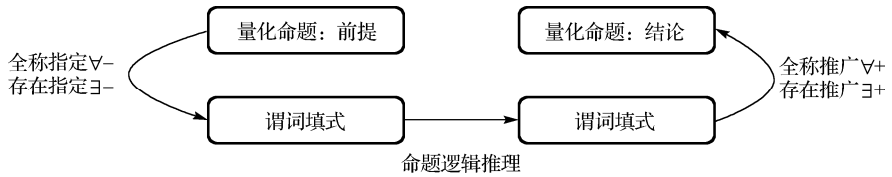
(4) **存在推广（产生）规则 EG**（Existence Generalization，或记为∃+）

若 $A(s)$ 为 1，则 $\exists xA(x)$ 为 1，即

$$\frac{\because \quad A(s)}{\therefore \exists xA(x)}$$

其中的 s 为论域中的某个个体，可以是特殊或任意的一个，但 x 不能与 A 中的其他个体名重复。

如此一来，谓词逻辑的一般推理方法是：



[辨析] 引入全称（存在）指定规则的目的是消去全称（存在）量词，引入全称（存在）推广量词的目的是产生全称（存在）量词。

[辨析] 当量词之前有否定联结词时不能指定到个体词。例如，$\neg\ \forall xA(x) \Rightarrow \neg\ A(s)$ 是错误的推理形式，s 不能肯定是泛指还是特指。此时，必须使用量词否定等值式将否定联结词移到量词之后才能使用上述规则。

3．谓词演算自然推理示例

例 2-12 三段论的形式证明。

(1) 苏格拉底三段论：人是要死的，苏格拉底是人。所以，苏格拉底是要死的。

证明 记 $M(x)$：x 是人，$D(x)$：x 是要死的，s：苏格拉底，原论断表示为：

$$\forall x(M(x) \to D(x)), M(s) \Rightarrow D(s)。$$

① $M(s)$	P	
② $\forall x(M(x)\to D(x))$	P	
③ $M(s)\to D(s)$	全称指定②	注：转换为谓词填式
④ $D(s)$	T①③ I	

“全称指定”可直接写为“US”或“∀-”。做全称指定时，必须指定到 s，才能建立与命题 $M(s)$的联系。此外，此证明结论就是谓词填式，不用再推广到量化形式。

(2)亚里士多德三段论：所有人都是必死的，希腊人都是人，所以希腊人都是必死的。

证明 记 $M(x)$：x 是人，$D(x)$：x 是必死的，$Greek(x)$：x 是希腊人，原论断表示为：

$$\forall x(M(x) \to D(x)), \forall x(Greek(x) \to M(x)) \Rightarrow \forall x(Greek(x) \to D(x))。$$

① $\forall x(Greek(x)\to M(x))$	P	
② $Greek(a)\to M(a)$	US②	注：转换为谓词填式

③ $\forall x(M(x)\rightarrow D(x))$　　P
④ $M(a)\rightarrow D(a)$　　US③　　注：转换为谓词填式
⑤ $Greek(a)\rightarrow D(a)$　　T②④ I　　注：命题逻辑推证
⑥ $\forall x(Greek(x)\rightarrow D(x))$　　UG⑤　　注：转换回量化形式

注意理解证明过程中是如何利用谓词填式将命题“搭接”在一起的。

例 2-13　证明 $\forall x(A(x)\rightarrow(B(x)\wedge C(x)))\wedge\exists x(A(x)\wedge D(x))\Rightarrow\exists x(D(x)\wedge C(x))$。

证明　这里采用另一种记号。

① $\exists x(A(x)\wedge D(x))$　　P
② $A(c)\wedge D(c)$　　∃-①　　注：转换到谓词填式
③ $\forall x(A(x)\rightarrow(B(x)\wedge C(x)))$　　P
④ $A(c)\rightarrow(B(c)\wedge C(c))$　　∀-③
⑤ $A(c)$　　T② I　　注：转换到命题逻辑推证
⑥ $D(c)$　　T② I
⑦ $B(c)\wedge C(c)$　　T④⑤ I
⑧ $C(c)$　　T⑦ I
⑨ $D(c)\wedge C(c)$　　T⑥⑧ I
⑩ $\exists x(D(x)\wedge C(x))$　　∃+⑨　　注：转换回量化形式

观察下述的另一个证明过程，它用如下步骤代替例中的前 4 个步骤：

① $\forall x(A(x)\rightarrow(B(x)\wedge C(x)))$　　P
② $A(c)\rightarrow(B(c)\wedge C(c))$　　∀-①　　注：转换到谓词填式
③ $\exists x(A(x)\wedge D(x))$　　P
④ $A(c)\wedge D(c)$　　∃-③

此过程与前述证明过程相比仅是次序变化，但完全错误。②中的 c 来自于全称指定，是泛指的任意一个，而③只能指定到特殊的个体 c' 而不能是 c，它违背了∃-规则的要求。

[辨析] 经验告诉我们，同时存在全称量词量化和存在量词量化时，通常应先进行存在指定（ES），再进行全称指定（US）。反之不可。

例 2-14　证明 $\forall x(P(x)\vee Q(x))\Rightarrow\forall xP(x)\vee\exists xQ(x)$。

证明　结论为析取式，这里采用反证法。

① $\neg(\forall xP(x)\vee\exists xQ(x))$　　P（附加前提）
② $\neg\forall xP(x)\wedge\neg\exists xQ(x)$　　T① E
③ $\neg\forall xP(x)$　　T② I
④ $\neg\exists xQ(x)$　　T② I
⑤ $\exists x\neg P(x)$　　T③ E
⑥ $\forall x\neg Q(x)$　　T④ E
⑦ $\neg P(c)$　　ES⑤
⑧ $\neg Q(c)$　　US⑥

⑨ $\forall x(P(x)\vee Q(x))$ P

⑩ $P(c)\vee Q(c)$ US⑨

⑪ $Q(c)$ T⑦⑩ I

⑫ $Q(c)\wedge \neg Q(c)$（矛盾） T⑧⑪ I

例 2-15 证明推断：所有学生要参加物理或化学考试，因此，若非都参加物理考试，一定有人参加化学考试。论域为学生集合。

证明 记 $P(x)$：x 参加物理考试，$C(x)$：x 参加化学考试，则符号化为：

$$\forall x(P(x)\vee C(x))\Rightarrow \neg\ \forall xP(x)\rightarrow \exists xC(x)。$$

由于结论为条件式，这里采用 CP 规则。

① $\neg\ \forall xP(x)$ P（附加前提）

② $\exists x\neg\ P(x)$ T① E

③ $\neg\ P(s)$ ES②

④ $\forall x(P(x)\vee C(x))$ P

⑤ $P(s)\vee C(s)$ US④

⑥ $C(s)$ T③⑤ I

⑦ $\exists xC(x)$ EG⑥

⑧ $\neg\ \forall xP(x)\rightarrow \exists xC(x)$ CP

例 2-16 证明下述论断：所有有理数都是实数，所有无理数也是实数，虚数不是实数。因此，虚数既不是有理数也不是无理数。

证明 记 $Q(x)$：x 是有理数，$N(x)$：x 是无理数，$R(x)$：x 是实数，$I(x)$：x 是虚数，可符号化为：

$\forall x(Q(x)\rightarrow R(x))$，$\forall x(N(x)\rightarrow R(x))$，$\forall x(I(x)\rightarrow \neg R(x))\Rightarrow \forall x(I(x)\rightarrow(\neg Q(x)\wedge \neg N(x)))$。

① $\forall x(I(x)\rightarrow \neg R(x))$ P

② $I(a)\rightarrow \neg R(a)$ US①

③ $\forall x(Q(x)\rightarrow R(x))$ P

④ $Q(a)\rightarrow R(a)$ US③

⑤ $\neg R(a)\rightarrow \neg Q(a)$ T④ E

⑥ $I(a)\rightarrow \neg Q(a)$ T②⑤ I

⑦ $\forall x(N(x)\rightarrow R(x))$ P

⑧ $N(a)\rightarrow R(a)$ US⑦

⑨ $\neg R(a)\rightarrow \neg N(a)$ T⑧ E

⑩ $I(a)\rightarrow \neg N(a)$ T②⑨ I

⑪ $I(a)\rightarrow(\neg Q(a)\wedge \neg N(a))$ T⑥⑩ I

⑫ $\forall x(I(x)\rightarrow(\neg Q(x)\wedge \neg N(x)))$ UG⑪

注意结论中的条件式是被量词约束的，不能采用 CP 规则论证。

例 2-17 证明下述论断：每一个大学生不是文科生就是理工科的，有的大学生是优等生，小

张不是文科生，但他是优等生。因此，如果小张是大学生，他就是理工科学生。

证明　记 $S(x)$：x 是大学生，$A(x)$：x 是文科学生，$E(x)$：x 是理工科学生，$T(x)$：x 是优等生，z：小张，可符号化为：

$$\forall x(S(x)\rightarrow(A(x)\vee E(x))),\ \exists x(S(x)\wedge T(x)),\ \neg A(z)\wedge T(z)\Rightarrow S(z)\rightarrow E(z)。$$

这个题目的很多条件是冗余的。由常识可知，优等生跟文理科学生毫不相干，对推理没有帮助。

① $\neg A(z)\wedge T(z)$　　P

② $\neg A(z)$　　T① I

③ $S(z)$　　P（附加前提）

④ $\forall x(S(x)\rightarrow(A(x)\vee E(x)))$　　P

⑤ $S(z)\rightarrow(A(z)\vee E(z))$　　US④

⑥ $A(z)\vee E(z)$　　T③⑤ I

⑦ $E(z)$　　T②⑥ I

⑧ $S(z)\rightarrow E(z)$　　CP

例 2-18　下面的推理过程正确吗？为什么？

(a) ① $\forall x(P(x)\rightarrow Q(x))$　　P

② $P(y)\rightarrow Q(y)$　　US①

③ $\exists xP(x)$　　P

④ $P(y)$　　ES③

⑤ $Q(y)$　　T②④ I

⑥ $\exists xQ(x)$　　EG⑤

(b) ① $P(x)\rightarrow Q(y)$　　P

② $\exists x(P(x)\rightarrow Q(x))$　　EG①

(c) ① $\forall x(P(x)\rightarrow Q(x))$　　P

② $P(t)\rightarrow Q(x)$　　US①

(d) ① $\exists xP(x)$　　P

② $P(c)$　　ES①

③ $\exists xQ(x)$　　P

④ $Q(c)$　　ES③

解　(a) 步骤④的存在指定到个体时，不能保证是 y。正确方法是调换步骤③、④和步骤①、②的顺序。

(b) 步骤①中的 x、y 是不同变元，不能推广为同一变元。

(c) 采用量词指定规则时，辖域中的同一变元必须指定到同一个个体。

(d) 存在量词指定时只能是特殊的个体。对于不同的存在量词量化命题，保证其成立的个体一般是不同的，不能指定到同一个个体。步骤④应为不同于 c 的名字，如 s。

思考与练习 2.5

2-25 说明下述推理中的错误。

(a) ① $\neg\exists x\big(p(x)\vee q(x)\big)$ P

② $p(y)\vee q(y)$ ES①

(b) ① $\forall x\big(p(x)\to q(y)\big)$ P

② $\forall x(p(x))\to q(y)$ T①E

(c) ① $\forall x(p(x)\vee q(x))$ P

② $p(a)\vee q(a)$ US①

③ $\exists x(p(x))$ P

④ $p(a)$ ES③

(d) ① $\forall x\exists yA(x,y)$ P

② $\exists yA(a,y)$ US①

③ $A(a,b)$ ES②

④ $\forall xA(x,b)$ UG③

⑤ $\exists y\forall xA(x,y)$ EG④

2-26 形式证明下列各式。

(a) $\forall x(\neg P(x)\to Q(x))$，$\forall x\neg Q(x)\Rightarrow\exists xP(x)$。

(b) $\exists xP(x)\to\forall xQ(x)\Rightarrow\forall x(P(x)\to Q(x))$。

(c) $\forall x(P(x)\to Q(x))\Rightarrow\forall xP(x)\to\forall xQ(x)$。

(d) $\forall x(P(x)\vee Q(x))\Rightarrow\forall xP(x)\vee\exists xQ(x)$。

(e) $\forall x(P(x)\to Q(x))$，$\forall x(R(x)\to\neg Q(x))\Rightarrow\forall x(R(x)\to\neg P(x))$。

(f) $\forall x(P(x)\vee Q(x))$，$\forall x(Q(x)\to\neg R(x))$，$\forall xR(x)\Rightarrow\forall xP(x)$。

2-27 符号化并形式证明下列推理过程。

(a) 有理数都是实数，有些有理数是整数，因此，有些实数是整数。

(b) 如果一个人喜欢步行就不喜欢骑马。每个人都喜欢骑马或乘车。有的人不爱乘车。因此，有的人不爱步行。

(c) 每个旅客都坐头等舱或二等舱，富裕的旅客坐头等舱，有的旅客富裕，有的不富裕。因此，有的旅客坐二等舱。

第 3 章　集合论基础

集合论是现代数学的基础，其概念出现在所有的数学分支中。集合论的开创性工作来自十九世纪末的德国数学家康托尔（Georg Cantor）。康托尔对任意元素的集合进行了深入研究，提出了关于基数、序数和良序集等理论，奠定了集合论的深厚基础。随着 1900 年前后出现的各种悖论，使人们意识到集合论中存在着漏洞，并促使集合论向公理化发展。1904～1908 年，策墨罗（Zermelo）提出了第一个集合论的公理系统，使集合论的矛盾得以解决，并逐步形成了公理化集合论与抽象集合论，集合理论得以完善。相对地，康托尔的集合论被称为朴素集合论，也是我们今天广泛使用的集合论。

在计算机领域中，集合几乎无处不在，尤其在数据结构、数据库、人工智能领域及程序设计语言等课程中，集合论有着重要的直接应用。

3.1　集合的概念与表示方法

3.1.1　集合描述

集合（set）是一个不能精确定义的概念，一些可区分的事物（对象）组成的整体就是**集合**。若 a 是组成集合 A 的事物，则 a 是集合 A 的元素，称作 a **属于** A，记作

$$a \in A \text{。}$$

否则，a 不是集合 A 的元素，称作 a **不属于** A，记作

$$a \notin A \text{。}$$

[辨析] $a \in A$ 和 $a \notin A$ 都是命题，即命题 $a \in A$ 为真，则 a 是集合 A 的元素；$a \notin A$ 为真，则 a 不是集合 A 的元素。$a \notin A \Leftrightarrow \neg(a \in A)$，或者说，$a \notin A$ 是 $\neg(a \in A)$ 的简单表示。

如果组成一个集合的元素个数是有限的，则称其为**有限（穷）集合**，否则称为**无限（穷）集合**。有限集合 A 的元素个数用 $|A|$ 表示。

集合有 2 种表示法。

1．枚举元素法

枚举元素法也称为“外延法”或“列举法”，是指直接列出集合的所有元素，如：

$$X = \{1, 2, 3\},$$

$$M = \{\text{花，水，空气}\}。$$

这种方法只能表示那些包含有限个元素的有限集。集合中可以包含任何对象，且集合的元素是无序的。

[延伸] 在程序设计语言中一般也采用这样的表示法。例如，C 语言中定义一个一维数组就构成了一个集合:

```
int  a[3] = {3, 2, 5};
```

与数学中的概念不同，集合 a 仅能包含类型相同（int 类型）的 3 个元素，且元素是有序的[1]。

2．描述法

描述法也称为“内涵法”或“叙述法”。如果集合中的元素性质相同或相近，可以用谓词 $p(x)$ 来刻画其性质，如令 $p(x)$：x 是奇数，则奇数集合可表示为：

$$A=\{x \mid p(x)\},$$

或者，

$$A=\{x \mid x\text{是奇数}\}。$$

上述表示法的含义是：对于任何一个个体 x_0，若谓词填式 $p(x_0)$为真，则 x_0 是 A 的元素，否则 x_0 不是 A 的元素。

集合的元素仍可以是集合，如 $A=\{a,\{a,b\},b\}$，此集合有 3 个元素，a、b 和集合$\{a,b\}$。

无论怎样表示，集合只注重其组成成分，元素既不重复，也无次序。

[外延性公理] 两个集合相等当且仅当它们有相同的元素。

外延性公理说明，只要两个集合的元素一样就是一个集合，只是外观不同。例如，下述三个集合是相同的：

$$\{1, 2, 3\},$$

$$\{2, 3, 1\},$$

$$\{x \mid x\text{是方程}(x-1)(x-2)(x-3)=0\text{的根}\}。$$

[辨析] 练习用谓词逻辑的观点看待集合，进而去严格推理，逐步将朴素的思维提升到严密的逻辑思维。

一些常用集合用固定字母表示，包括：自然数集 $\mathbf{N}=\{0, 1, 2, \cdots\}$，整数集 $\mathbf{Z}=\mathbf{I}=\{\cdots, -2, -1, 0, 1, 2, \cdots\}$，正整数集 $\mathbf{Z}^+=\mathbf{I}^+=\{1, 2, \cdots\}$，有理数集 $\mathbf{Q}=\{p/q \mid p\in\mathbf{Z}, q\in\mathbf{Z}$ 且 $q\neq 0\}$，实数集 $\mathbf{R}$，正实数集 $\mathbf{R}^+$，复数集 $\mathbf{C}$ 等。

3.1.2 集合的包含与相等

1．子集与集合包含

[定义 3-1] 如果集合 A 的每个元素都是集合 B 的元素，称集合 A 是集合 B 的**子集**（subset），或集合 A **包含于**集合 B，记作 $A\subseteq B$。用谓词符号表示为：

$$A\subseteq B \Leftrightarrow \forall x(x\in A\rightarrow x\in B)。$$

由定义，对任意的集合 A，显然有 $A\subseteq A$。

这是一个至关重要的核心定义，用自然语言应描述为：对每个 x，只要 $x \in A$，则 $x \in B$。

[辨析] “包含于”不是“包含”，二者恰好相反。它们都可以被理解成关系运算。

[辨析] 概念成立的要求是“对每个元素”或“对所有的元素”而不是“存在一个或一些”，即定义要用全称量词而不是存在量词来刻画。这种对全部数量的要求体现在绝大多数定义中。

[定理 3-1] 对任意的集合 A、B、C，若 $A \subseteq B$ 且 $B \subseteq C$，则 $A \subseteq C$。

证明　对 $\forall x \in A$，由 $A \subseteq B$，有 $x \in B$。又因为 $B \subseteq C$，有 $x \in C$，故 $A \subseteq C$。

[辨析] 上述性质与“$a \leqslant b$ 且 $b \leqslant c$，则 $a \leqslant c$”一致，称为包含于关系 $\subseteq$ 具有“传递性”。

[定理 3-2] 两集合相等的充分必要条件是它们互为子集，即互相包含，符号表示为：

$$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A \Leftrightarrow \forall x(x \in A \leftrightarrow x \in B)。$$

证明　若集合 A=B，则二者有相同的元素，故 $\forall x(x \in A \rightarrow x \in B)$ 与 $\forall x(x \in B \rightarrow x \in A)$ 均为真，有 $A \subseteq B$ 且 $B \subseteq A$。

若集合 A 与 B 互为子集，如果 $A \neq B$，则 $\exists x(x \in A \wedge x \notin B)$ 为真，或 $\exists x(x \in B \wedge x \notin A)$ 为真。因为

$$\exists x(x \in A \wedge x \notin B) \Leftrightarrow \exists x \neg(\neg\, x \in A \vee x \in B) \Leftrightarrow \neg\ \forall x(x \in A \rightarrow x \in B)\ ,$$
$$\exists x(x \in B \wedge x \notin A) \Leftrightarrow \exists x \neg(\neg\, x \in B \vee x \in A) \Leftrightarrow \neg\ \forall x(x \in B \rightarrow x \in A)\ 。$$

故 $A \subseteq B$ 为假或 $B \subseteq A$ 为假，与假定矛盾，结论成立。

这是集合论中最核心的定理，是证明集合相等的根本方法。

[辨析] 两数 a 和 b 相等描述为 $a \leqslant b$ 且 $b \leqslant a$，两集合 A 和 B 相等描述为 $A \subseteq B$ 且 $B \subseteq A$，可见运算 $\subseteq$ 与 $\leqslant$ 有类似的含义。

2．真子集

[定义 3-2] 如果集合 A 的每个元素都是集合 B 的元素，但集合 B 中至少有一个元素不属于 A，称集合 A 是集合 B 的**真子集**（proper subset），或集合 A **严格包含于**（**真包含于**）集合 B，记作 $A \subset B$。符号表示为：

$$A \subset B \Leftrightarrow \forall x(x \in A \rightarrow x \in B) \wedge \exists x(x \in B \wedge x \notin A) \Leftrightarrow A \subseteq B \wedge A \neq B。$$

例如，集合 $\{a,b\}$ 是 $\{a,b,c\}$ 的子集，也是真子集。

[辨析] 定义中的“集合 B 中至少有一个元素不属于 A”也可说成“A 不等于 B”。

3.1.3　空集与全集

1．空集

[定义 3-3] 不包含任何元素的集合称为**空集**，记作 Ø。符号表示为：

$$\text{Ø} = \{x \mid p(x) \wedge \neg\, p(x)\}\ ,\ p(x) \text{是任意谓词。}$$

[辨析] 对任意的个体 x，命题 $x \in \text{Ø}$ 恒为 0，即该命题为永假式。

[辨析] $\text{Ø} \neq \{0\}$，$\text{Ø} \neq \{\text{Ø}\}$。Ø 表示没有任何对象。如果把集合看作一个文件夹，Ø 就是不包含任何文件的空文件夹。

显然，若 $A \neq \varnothing$，则命题 $\exists x(x \in A)$ 为真。

[定理 3-3] 对任意的集合 A，有 $\varnothing \subseteq A$，即空集是所有集合的子集。

证明 由于空集没有任何元素，通常用反证法证明。

若 $\varnothing \subseteq A$ 为假，则 $\neg\ \forall x(x \in \varnothing \to x \in A)$ 为真。因为，

$$\neg\ \forall x(x \in \varnothing \to x \in A) \Leftrightarrow \exists x \neg(\neg\ x \in \varnothing \vee x \in A) \Leftrightarrow \exists x(x \in \varnothing \wedge x \notin A)$$

$$\Leftrightarrow \exists x(x \in \varnothing) \wedge \exists x(x \notin A) \Rightarrow \exists x(x \in \varnothing)。$$

说明 $\exists x(x \in \varnothing)$ 为真。这与空集的定义矛盾。

在集合论中，大量的问题仅是对一个概念是否成立的判定，而这又取决于判定描述此概念的条件命题是否为真。这是学习时需要掌握的核心技术。对于定理 3-3，要证明 $\varnothing \subseteq A$ 成立，只要说明 $\forall x(x \in \varnothing \to x \in A)$ 为真。于是，也可以不采用反证法证明：

对 $\forall x$，由于 $x \in \varnothing$ 为永假式，故

$$\forall x(x \in \varnothing \to x \in A) \Leftrightarrow\ \forall x(0 \to x \in A) \Leftrightarrow \forall x(1) \Leftrightarrow 1。$$

于是，$\varnothing \subseteq A$ 成立。

可见，任意集合 $A \neq \varnothing$ 均有两个子集，分别是 $\varnothing$ 和 A。

2．全集

[定义 3-4] 在一定范围内，包含所有元素的集合称为**全集**，记作 U（universal set，或 E）。符号表示为：

$$U = \{x \mid p(x) \vee \neg\ p(x)\}，\ p(x)是任意谓词。$$

对任意的对象 x，命题 $x \in U$ 恒为 1，即该命题为永真式。

对任意的集合 A，有 $A \subseteq U$。

[辨析] 空集是绝对的概念，全集则是相对的概念，即只要涵盖所讨论对象的集合就可以作为全集，而并非需要包括世间万物。

[延伸] 悖论体现了逻辑上的不一致性，可以由集合反映出来。例如，把所有集合分为 2 类，第一类中的集合以其自身为元素，第二类中的集合不以自身为元素。令第二类集合所组成的集合为 Q，有：

$$Q = \{A \mid A \notin A\}。$$

那么，无论说 $Q \in Q$ 还是 $Q \notin Q$ 都会产生矛盾，即不能说明 $Q \in Q$ 的真假。这就是集合论悖论（罗素悖论）。

在信息领域处理的实际问题中，都有一个明确甚至有限的全集，不会产生悖论[19]。因此，本课程仍然介绍朴素集合论而非公理集合论。

利用下述示例可以帮助我们正确理解属于 $\in$ 和包含于 $\subseteq$ 的含义。

例 3-1 构造集合 A、B 和 C，使 $A \in B$，$B \in C$，且 $A \notin C$。

解 令 $A = \{a\}$，$B = \{\{a\}, b\}$，$C = \{\{\{a\}, b\}, c\}$ 则满足要求。

为了消除括号带来的混乱，可写成：

$A=\{a\}$，　$B=\{A,b\}$，　$C=\{B,c\}$。

这更能体会出构造者的想法。

例 3-2　对任意集合 A、B 和 C，确定下述命题是否为真。

(a) 如果 $A\in B$ 及 $B\subseteq C$，则 $A\in C$。　　(b) 如果 $A\in B$ 及 $B\subseteq C$，则 $A\subseteq C$。

(c) 如果 $A\subseteq B$ 及 $B\in C$，则 $A\in C$。　　(d) 如果 $A\subseteq B$ 及 $B\in C$，则 $A\subseteq C$。

(e) 如果 $A\subseteq B$ 及 $B\nsubseteq C$，则 $A\notin C$。　　(f) 如果 $A\subseteq B$ 及 $B\in C$，则 $A\notin C$。

(g) 如果 $A\subseteq B$ 则 $A\notin B$。

解 (a) 真。因为 B 是 C 的子集，故 B 的元素 A 也是 C 的元素。

(b) 假。如 $A=\{a\}$，　$B=\{A\}$，　$C=\{A,c\}$。

(c) 假。如 $A=\{a\}$，　$B=\{a,b\}$，　$C=\{B,c\}$。

(d) 假。反例同(c)。

(e) 假。如 $A=\{a\}$，　$B=\{a,b\}$，　$C=\{A,c\}$。

(f) 假。如 $A=\{a\}$，　$B=\{a,b\}$，　$C=\{A,B\}$。

(g) 假：如 $A=\{a\}$，　$B=\{a,A\}$。

3.1.4　集合的幂集

[定义 3-5]　集合 A 的所有子集构成的集合称为 A 的**幂集**（power set），记作

$$\mathscr{P}(A)=\{x\mid x\subseteq A\}。$$

例如，$\mathscr{P}(\varnothing)=\{\varnothing\}$。若 $A=\{a,b,c\}$，则

$$\mathscr{P}(A)=\{\varnothing,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},\{a,b,c\}\}。$$

不同子集含有的元素个数不同，在计算机内表示起来困难，也难以存储和运算。一个更有效的方法是将其表示为定长的串。若 $A=\{a_1,a_2,\cdots,a_n\}$，其所有子集可表示为：

$$A_{x_1x_2\cdots x_n}。$$

其中，

$$x_i=\begin{cases}1\ ,a_i\in A\\0\ ,a_i\notin A\end{cases},\quad 1\leqslant i\leqslant n。$$

例如，前述的幂集可写成

$$\mathscr{P}(A)=\{A_{000},A_{100},A_{010},A_{001},A_{110},A_{101},A_{011},A_{111}\}。$$

如果用十进制表示，其子集为 A_0～A_7。

这种对子集的编码表示方法十分有效。例如，若 $|A|$ 不超过 8，可以用一个字节的量存储 A 的子集，每个二进制位标志着对应的元素是否属于此子集。

[延伸] 利用程序设计语言中的位运算即可完成对编码子集的运算。例如，要计算子集 $A_{10010010}$ 和 $A_{01000010}$ 的交集，只需要对两个单字节的整数（机器内部为二进制串）10010010 和 01000010

做按位与运算&，得到子集 $A_{00000010}$。类似地，两个子集的并、对称差可分别由按位或运算|和按位异或运算^直接计算出来[1]。

通过子集的编码表示还可以很容易得到全部子集的数量，即幂集的元素个数。

[定理 3-4] 若 $|A|=n$，则 $|\mathscr{P}(A)|=2^n$。

因为任何一个码字 x_i 只有 1 或 0 两种取值，故 n 个码字的总取值数量为：

$$\underbrace{\binom{2}{1}\binom{2}{1}\cdots\binom{2}{1}}_{n\text{个}}=2^n。$$

还存在另一种计算幂集元素个数的方法。因为 n 个元素中取 k 个元素有 $\binom{n}{k}$ 种取法，$\mathscr{P}(A)$ 的元素个数为 $\sum_{k=0}^{n}\binom{n}{k}$。由二项式展开式

$$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^n y^{n-k}。$$

令 x 和 y 为 1 即知结论成立。

[辨析] 空集的幂集只有一个元素，其他集合的幂集有偶数个元素。

由于一个集合 X 的幂集 $\mathscr{P}(X)$ 有 $2^{|X|}$ 个元素，故也用 2^X 表示集合 X 的幂集。

例 3-3 求出集合 A 的幂集。

(1) $A=\{a,\{a\}\}$。　　(2) $A=\{\{1,\{2,3\}\}\}$。

(3) $A=\{\varnothing,a,\{b\}\}$。　　(4) $A=\mathscr{P}(\varnothing)$。

解 (1) 集合 A 有 2 个元素，$\mathscr{P}(A)=\{\varnothing,\{a\},\{\{a\}\},\{\{a,\{a\}\}\}\}=\{\varnothing,\{a\},\{\{a\}\},A\}$。

(2) 集合 A 有 1 个元素，$\mathscr{P}(A)=\{\varnothing,\{\{1,\{2,3\}\}\}\}=\{\varnothing,A\}$。

(3) 集合 A 有 3 个元素，$\mathscr{P}(A)=\{\varnothing,\{\varnothing\},\{a\},\{\{b\}\},\{\varnothing,a\},\{\varnothing,\{b\}\},\{a,\{b\}\},A\}$。

(4) $\mathscr{P}(A)=\mathscr{P}(\mathscr{P}(\varnothing))=\mathscr{P}(\{\varnothing\})=\{\varnothing,\{\varnothing\}\}$。

思考与练习 3.1

3-1 准确说明并用符号描述 $A\subseteq B$、$A\subset B$、$A=B$ 的含义。

3-2 利用基本定义推出 $A\nsubseteq B$、$A\not\subset B$、$A\neq B$ 定义的符号描述。

3-3 何谓集合 A 的幂集？对于有限集，其幂集的元素个数是多少？

3-4 举出使下述命题成立的例子。

(a) $A\in B$，$B\in C$，但 $A\notin C$。　　(b) $A\in B$ 且 $A\subseteq B$。

3-5 确定下述命题的真伪。

(a) $\varnothing\subseteq\varnothing$。　　(b) $\varnothing\in\varnothing$。

(c) $\varnothing \in \{\varnothing\}$。　(d) $\{a,b\} \subseteq \{a,b,c,\{a,b,c\}\}$。

(e) $\{a,b\} \in \{a,b,c,\{a,b,c\}\}$。

3-6　对任意的集合 A、B、C，证明或否定下述推断。

(a) 若 $A \in B$ 且 $B \in C$，则 $A \in C$。　(b) 若 $A \in B$ 且 $B \subseteq C$，则 $A \in C$。

(c) 若 $A \in B$ 且 $B \nsubseteq C$，则 $A \notin C$。　(d) 若 $A \subseteq B$ 且 $B \nsubseteq C$，则 $A \notin C$。

3-7　求下列集合的幂集。

(a) $\{a, \{a\}\}$。　(b) $\{\{a, \{b, c\}\}\}$。

(c) $\{\varnothing, 1, \{2\}\}$。　(d) $\mathscr{P}(\mathscr{P}(\varnothing))$。

3-8　记 $T=\mathscr{P}(\mathscr{P}(\mathscr{P}(\varnothing)))$，判别是否有：$\varnothing \in T$、$\varnothing \subseteq T$、$\{\varnothing\} \in T$、$\{\varnothing\} \subseteq T$、$\{\{\varnothing\}\} \in T$ 和 $\{\{\varnothing\}\} \subseteq T$？

3-9　设 $A = \{a_1, a_2, \cdots, a_8\}$，问 A_{17} 和 A_{33} 表示的子集是什么？子集 $\{a_2, a_3, a_7\}$ 和 $\{a_5, a_8\}$ 又是如何编码的？

3-10　设 A、B 为任意集合，证明：$A = B$ 当且仅当 $\mathscr{P}(A) = \mathscr{P}(B)$。

3.2　集 合 运 算

3.2.1　基本运算

集合运算是由已知集合得到新集合的手段。

1．集合的交（intersection）

[定义 3-6] 集合 A 和 B 的所有共同元素组成的集合称为 A 与 B 的**交**，记作 $A \cap B$。符号表示为：

$$A \cap B = \{x | x \in A \wedge x \in B\}。$$

例如，$\{1,2,3\} \cap \{2,1,-1\} = \{1,2\}$，$\{1,3\} \cap \varnothing = \varnothing$，$\{1,3\} \cap U = \{1,3\}$。

[理解] (1) 只要 $x \in A$ 且 $x \in B$，必有结论 $x \in A \cap B$；(2) 只要 $x \in A \cap B$，必有结论 $x \in A$ 且 $x \in B$，即 $x \in A \wedge x \in B$ 为真。也可换个说法：若 $x \in A_1 \cap A_2$，则 $\forall i(1 \leqslant i \leqslant 2 \wedge i \in \mathbf{Z} \to x \in A_i)$ 为真，或者说，$\forall i((i = 1 \vee i = 2) \to x \in A_i)$ 为真。

若 $A \cap B = \varnothing$，称集合 A 与 B 是**不相交**的。

2．集合的并（union）

[定义 3-7] 属于集合 A 或者属于集合 B 的所有元素组成的集合称为 A 与 B 的**并**，记作 $A \cup B$。符号表示为：

$$A \cup B = \{x | x \in A \vee x \in B\}。$$

例如，$\{1,2,3\} \cup \{2,1,-1\} = \{1,2,3,-1\}$，$\{1,3\} \cup \varnothing = \{1,3\}$，$\{1,3\} \cup U = U$。

[理解] (1) 只要 $x \in A$ 或者 $x \in B$，必有结论 $x \in A \cup B$；(2) 只要 $x \in A \cup B$，必有结论 $x \in A$ 或者 $x \in B$，即 $x \in A \vee x \in B$ 为真。也可换个说法：若 $x \in A_1 \bigcup A_2$，则 $\exists i(1 \leqslant i \leqslant 2 \wedge i \in \mathbf{Z} \wedge x \in A_i)$ 为真，或者说，$\exists i((i=1 \vee i=2) \wedge x \in A_i)$ 为真。

3．集合的差（difference，subtraction）

[定义 3-8] 属于集合 A 而不属于集合 B 的所有元素组成的集合称为集合 A 与 B 的**差**，记作 $A-B$。符号表示为：

$$A-B=\{x|x \in A \wedge x \notin B\}=\{x|x \in A \wedge \neg\, x \in B\}。$$

[理解] (1) 只要 $x \in A$ 且 $x \notin B$，必有结论 $x \in A-B$；(2) 只要 $x \in A-B$，必有结论 $x \in A$ 且 $x \notin B$；(3) 只要 $x \in A$ 且 $x \in B$，必有结论 $x \notin A-B$。

对于一般集合，$A-B$ 也称为 B 对于 A 的**补**或**相对补**，$U-B$ 称为 B 的**绝对补**或 B 的**余集**，简记为 $\sim B$ 或 $\overline{B}$。

[辨析] 依定义，$\sim B=U-B=\{x \mid x \in U \wedge x \notin B\}=\{x \mid 1 \wedge \neg\, x \in B\}=\{x \mid \neg\, x \in B\}$，即 $\sim B$ 是由所有不属于 B 的元素组成的集合。于是，有

$$A-B=\{x|x \in A \wedge \neg\, x \in B\}=A \bigcap \sim B。$$

例 3-4 若 A 为素数集合，B 为奇数集合，求 $A-B$。

解 $A-B=\{2\}$。

4．集合的对称差（symmetric difference）

[定义 3-9] 属于集合 A 或者属于集合 B，但不同时属于 A 和 B 的所有元素组成的集合称为集合 A 与 B 的**对称差**，记作 $A \oplus B$。符号表示为：

$$\begin{aligned} A \oplus B &= (A \bigcup B)-(A \bigcap B)=\{x \mid x \in A \bigcup B \wedge x \notin A \bigcap B\} \\ &= (A-B) \bigcup (B-A) \\ &= \{x|x \in A \bar{\vee} x \in B\}。 \end{aligned}$$

[理解] (1) 只要 $x \in A$ 或 $x \in B$，且 $x \notin A \bigcap B$，必有结论 $x \in A \oplus B$；(2) 只要 $x \in A \oplus B$，必有结论 $x \in A$ 或 $x \in B$，且 $x \notin A \bigcap B$；(3) 只要 $x \in A \wedge x \in B$，必须 $x \notin A \oplus B$。

例 3-5 确定以下各式的值：

$\varnothing \bigcap \{\varnothing\}$，$\{\varnothing\} \bigcap \{\varnothing\}$，$\varnothing \bigcup \{\varnothing\} \bigcup \{\{\varnothing\}\}$，$\{\varnothing,\{\varnothing\}\}-\varnothing$，$\{\varnothing,\{\varnothing\}\}-\{\varnothing\}$，$\{\varnothing,\{\varnothing\}\}-\{\{\varnothing\}\}$，$\{\varnothing,\{\varnothing\}\} \oplus \{\{\varnothing\}\}$。

解 $\varnothing \bigcap \{\varnothing\}=\varnothing$，$\{\varnothing\} \bigcap \{\varnothing\}=\{\varnothing\}$，$\varnothing \bigcup \{\varnothing\} \bigcup \{\{\varnothing\}\}=\{\varnothing,\{\varnothing\}\}$，

$\{\varnothing,\{\varnothing\}\}-\varnothing=\{\varnothing,\{\varnothing\}\}$，$\{\varnothing,\{\varnothing\}\}-\{\varnothing\}=\{\{\varnothing\}\}$，

$\{\varnothing,\{\varnothing\}\}-\{\{\varnothing\}\}=\{\varnothing\}$，$\{\varnothing,\{\varnothing\}\} \oplus \{\{\varnothing\}\}=\{\varnothing\}$。

[辨析] 直观理解基本运算的有效技术是英国数学家 John Venn 在 1881 年给出的文氏图（维恩图）。用一个矩形表示全集 U，内部用圆表示集合，用点表示集合的元素，如图 3-1 所示，其中，阴影部分显示了集合运算的结果。

考虑到运算的封闭性，通常将集合运算放在一个幂集上来考虑。例如，对于任意的集合 S，可以在其幂集 $\mathscr{P}(S)$ 上讨论集合的运算。这样一来，S 就是全集，对任意的 $x \in \mathscr{P}(S)$，$y \in \mathscr{P}(S)$，集合 x 与 y 的运算结果 z 仍是 S 的子集，即 $z \in \mathscr{P}(S)$。

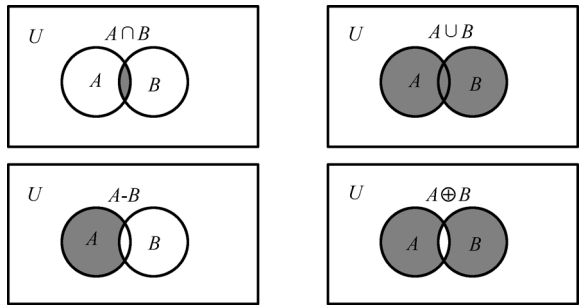


图 3-1

3.2.2　多集合的交与并

1．多个集合的交

[定义 3-10] 所有集合 $A_i(1 \leqslant i \leqslant n)$的共同元素组成的集合称为 A_i 的**交**，记作 $\bigcap_{i=1}^{n} A_i$。符号表示为：

$$\bigcap_{i=1}^{n} A_i = \{x \mid \forall i(1 \leqslant i \leqslant n \rightarrow x \in A_i)\}。$$

尽管定义中没有体现，容易理解，i 应为整数。当然，也可以在定义中明确指出。

[理解] 若有 $x \in \bigcap_{i=1}^{n} A_i$，则对$\forall i$，只要 $1 \leqslant i \leqslant n$，则 $x \in A_i$。

2．多个集合的并

[定义 3-11] 至少属于某个集合 A_i（$1 \leqslant i \leqslant n$）的元素组成的集合称为 A_i 的**并**，记作 $\bigcup_{i=1}^{n} A_i$。符号表示为：

$$\bigcup_{i=1}^{n} A_i = \{x \mid \exists i(1 \leqslant i \leqslant n \wedge x \in A_i)\}。$$

[理解] 若有 $x \in \bigcup_{i=1}^{n} A_i$，则$\exists i$，$1 \leqslant i \leqslant n$，使 $x \in A_i$。

如果将定义中的 n 改为 $+\infty$，就是无穷个集合的交与并。

例如，记 $A_i = \{1, 1/2, 1/3, \cdots, 1/i\}$，则 $\bigcap_{i=1}^{+\infty} A_i = \{1\}$，$\bigcup_{i=1}^{+\infty} A_i = \{1/i \mid i \geqslant 1 \wedge i \in \mathbf{Z}\}$。

3．集合的广义交与并

[定义 3-12] 设集合$\mathcal{A}$的元素为集合，所有$\mathcal{A}$的元素的共同元素组成的集合称为$\mathcal{A}$的“**广义交**”，记作$\bigcap\mathcal{A}$。符号表示为：

$$\bigcap\mathcal{A} = \{x \mid \forall z(z \in \mathcal{A} \rightarrow x \in z)\}。$$

很明显，若有 $x \in \bigcap\mathcal{A}$，则对 $\forall z \in \mathcal{A}$，必有 $x \in z$。

[定义 3-13] 设集合$\mathcal{A}$的元素为集合，属于$\mathcal{A}$的某个元素的元素组成的集合称为$\mathcal{A}$的**“广义并”**，记作$\bigcup\mathcal{A}$。符号表示为：

$$\bigcup\mathcal{A}=\{x\mid\exists z(z\in\mathcal{A}\wedge x\in z)\}。$$

很明显，若有$x\in\bigcup\mathcal{A}$，则$\exists z\in\mathcal{A}$，且$x\in z$。

通俗地讲，集合$\mathcal{A}$的广义交和广义并就是$\mathcal{A}$的所有元素（集合）的交和并。

例 3-6 若$\mathcal{A}=\{\{a,b,c\},\{b,c,d\},\{a,c\}\}$，求$\bigcap\mathcal{A}$和$\bigcup\mathcal{A}$。

解

$$\bigcap\mathcal{A}=\{a,b,c\}\bigcap\{b,c,d\}\bigcap\{a,c\}=\{c\}，$$

$$\bigcup\mathcal{A}=\{a,b,c\}\bigcup\{b,c,d\}\bigcup\{a,c\}=\{a,b,c,d\}。$$

在一般科技文献中，多集合的交与并可以有各种灵活的记法。例如，$\bigcap_{i=1}^{n}A_i$和$\bigcup_{i=1}^{n}A_i$可以表示为：

$\bigcap_{1\leqslant i\leqslant n}A_i$，或$\bigcap_{i\in\{1,2,\cdots,n\}}A_i$，或$\bigcap_{i\in X}A_i$，$X=\{1,2,\cdots,n\}$。

$\bigcup_{1\leqslant i\leqslant n}A_i$，或$\bigcup_{i\in\{1,2,\cdots,n\}}A_i$，或$\bigcup_{i\in X}A_i$，$X=\{1,2,\cdots,n\}$。

又如，记 H、G 为集合，$aH=\{a\times h\mid h\in H\}$，则$\bigcup_{a\in G}aH=\bigcup\{aH\mid a\in G\}$代表了一种集合的广义并。若 H={0,1,2}，G={1,2,3}，则

$$\bigcup_{a\in G}aH=\bigcup_{a=1}^{3}aH=1H\bigcup 2H\bigcup 3H=\{0,1,2\}\bigcup\{0,2,4\}\bigcup\{0,3,6\}=\{0,1,2,3,4,6\}。$$

熟悉多集合运算的表示方法有利于对实际问题进行更准确的数学描述。

[延伸] 一种直接利用集合基本运算所产生的应用技术称为“数学形态学”，它在图像处理领域的图像分割、特征抽取、边缘检测、图像滤波、图像增强和恢复等方面都有广泛的用途[20-22]。例如，对于一幅二值（黑白）图像，其数据可描述成一个 0（黑）、1（白）组成的集合，记作 A。令 B 是一个小的图像集合，称为“结构元素”或“探针”。于是，可以定义如下的形态学运算:

$$A\ominus B=\{x\mid B+x\subset A\}，\ A\oplus B=\bigcup\{A+b\mid b\in B\}。$$

它们分别称为“腐蚀”和“膨胀”。$A\ominus B$ 是将 B 平移 x 后仍包含于 A 的所有 x 组成的集合，$A\oplus B$ 的定义采用了集合的广义并，含义是将 A 依据 B 的全部元素平移后产生的所有元素集合。这些运算作用到集合后就会产生如其名字所体现的作用。例如，图 3-2 是利用一个圆形的小结构元素 B 腐蚀一个矩形图像 A 的结果。

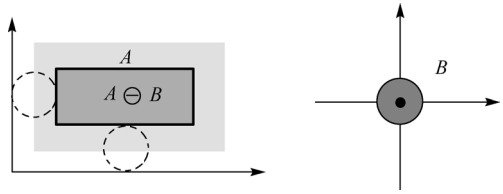


图 3-2

显然，原始图像 A 被腐蚀掉了边界。通过这种运算可以消除图像中的杂点、毛刺等噪声。类似地，通过膨胀可以添补图像中的小孔洞等成分。在此基础上，可以进一步定义开、闭、击中、击不中等运算。本质上，数学形态学是一种对信号的滤波。

思考与练习 3.2

3-11　说明并用符号描述 $A\cap B$、$A\cup B$、$A-B$、$\sim A$ 和 $A\oplus B$ 的含义。

3-12　设 $A=\{x|x$ 是 book 中的字母$\}$，$B=\{x|x$ 是 blood 中的字母$\}$，求 $A\cap B$、$A\cup B$、$A-B$ 和 $A\oplus B$。

3-13　设有自然数集 **N** 的子集 $A=\{i|i$ 可被 3 整除$\}$，$B=\{i|i$ 可被 5 整除$\}$，求 $A\cap B$、$A\cup B$、$\sim A$、$\sim(A\cap B)$。

3-14　若 $x\in A\cup B\cup C$，可以得到什么结论？若 $x\in A\cap B\cap C$，可以得到什么结论？用符号形式描述。

3-15　由 $x\in\bigcup_{i=1}^{+\infty}A_i$ 和 $x\in\bigcap_{i=1}^{+\infty}A_i$ 分别能得到什么结论？用符号形式描述。

3-16　对任意的正整数 i 和下述集合，求 $\bigcup_{i=1}^{+\infty}A_i$ 和 $\bigcap_{i=1}^{+\infty}A_i$。

(a) $A_i=\{i,i+1,i+2,\cdots\}$。　(b) $A_i=\{0,i\}$。

(c) $A_i=\{x\mid x\in\mathbf{R}\wedge 0<x<i\}$。　(d) $A_i=\{x\mid x\in\mathbf{R}\wedge x>i\}$。

3-17　有集合 $\varnothing\cup\{\varnothing\}$、$\{\varnothing\}\cap\{\varnothing\}$、$\{\varnothing,\{\varnothing\}\}-\{\varnothing\}$ 和 $\{\varnothing,\{\varnothing\}\}-\{\{\varnothing\}\}$，哪个集合的值不等于 $\{\varnothing\}$？

3-18　根据定义总结 $\cap$、$\cup$ 运算满足的算律。

3-19　$\oplus$ 运算满足哪些算律？$A\oplus A=$？$A\oplus\varnothing=$？$A\oplus U=$？

3-20　设 A、B 为集合，若 $A-B=B$，A 与 B 有何关系？若 $A-B=A$，A 与 B 有何关系？

3-21　设 A、B、C 为集合，判断下列命题的真假。若为真予以证明，否则给出反例。

(a) $A\subseteq B$ 当且仅当 $A\cup B=B$。　(b) $A\subseteq B$ 当且仅当 $A\cup(B-A)=B$。

(c) $A\subseteq B$ 当且仅当 $A\cap B=A$。　(d) $B\subseteq A$ 当且仅当 $(A-B)\cap B=A$。

3-22　对任意集合 A、B、C，下述命题是否成立？为什么？

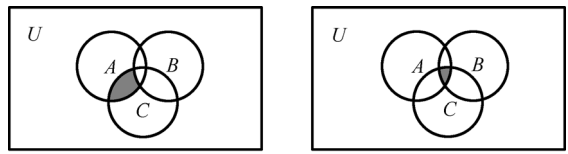
(a) $A\cup B=A\cup C$ 则 $B=C$。　(b) $A\cap B=A\cap C$ 则 $B=C$。

3-23　画出下述集合的文氏图。

(a) $\sim A\cap\sim B$。　(b) $A-\overline{(B\cup C)}$。

(c) $A\cap(\sim B\cup C)$。

3-24　用集合运算公式表示出图 3-3 中的阴影部分。



(a)　(b)

图 3-3

3-25　设集合 $\mathcal{A}=\{\{\varnothing,\{\varnothing\}\},\{\varnothing,\{\varnothing\},\{\{\varnothing\}\}\},\{\varnothing,\{\{\varnothing\}\}\}\}$，求 $\cap\mathcal{A}$ 和 $\cup\mathcal{A}$。

3.3 集合运算的性质与证明方法

集合运算满足很多与命题演算一致的性质。除了简单的集合元素计算（包括幂集）之外，集合的基本运算中几乎仅需要证明一个问题：集合包含。一个问题可能要求直接说明集合包含，也可能要求说明集合相等，但本质上都是集合包含，只是相等时要证明互相包含。

集合包含或相等有两种主要证明方法，其一是集合的恒等变换，其二是基于定义的推理。应深入理解第二种方法。

3.3.1 集合运算的性质与演算证明

可以通过化简、变形等运算证明集合包含或相等关系，从而得到一些基本算律。这些算律可视为集合运算的基本性质。

由于集合运算的定义来自于命题逻辑和谓词逻辑，基本算律和性质都与命题逻辑的算律完全相同，如交换律、结合律和分配律等。因此，可以从命题逻辑的基本等价式直接推断出集合运算的对应性质，参见表 3-1。

表 3-1

集合运算律	对应的命题等价关系	含　义
$A\cup\varnothing=A$ $A\cap E=A$	$a\vee 0\Leftrightarrow a$ $a\wedge 1\Leftrightarrow a$	同一律
$A\cup U=U$ $A\cap\varnothing=\varnothing$	$a\vee 1\Leftrightarrow 1$ $a\wedge 0\Leftrightarrow 0$	零律
$A\cup A=A$ $A\cap A=A$	$a\vee a\Leftrightarrow a$ $a\wedge a\Leftrightarrow a$	等幂律
$\sim(\sim A)=A$	$\neg(\neg a)\Leftrightarrow a$	对合律（补集律）
$A\cup B=B\cup A$ $A\cap B=B\cap A$	$a\vee b\Leftrightarrow b\vee a$ $a\wedge b\Leftrightarrow b\wedge a$	交换律
$A\cup(B\cup C)=(A\cup B)\cup C$ $A\cap(B\cap C)=(A\cap B)\cap C$	$a\vee(b\vee c)\Leftrightarrow(a\vee b)\vee c$ $a\wedge(b\wedge c)\Leftrightarrow(a\wedge b)\wedge c$	结合律
$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$ $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$	$a\wedge(b\vee c)\Leftrightarrow(a\wedge b)\vee(a\wedge c)$ $a\vee(b\wedge c)\Leftrightarrow(a\vee b)\wedge(a\vee c)$	分配律
$\sim(A\cup B)=\sim A\cap\sim B$ $\sim(A\cap B)=\sim A\cup\sim B$	$\neg(a\vee b)\Leftrightarrow\neg a\wedge\neg b$ $\neg(a\wedge b)\Leftrightarrow\neg a\vee\neg b$	德• 摩根律
$A\cup(A\cap B)=A$ $A\cap(A\cup B)=A$	$a\vee(a\wedge b)\Leftrightarrow a$ $a\wedge(a\vee b)\Leftrightarrow a$	吸收律
$A\cup\sim A=U$ $A\cap\sim A=\varnothing$	$a\vee\neg a\Leftrightarrow 1$ $a\wedge\neg a\Leftrightarrow 0$	否定律

利用各运算的定义能够直接验证上述算律中的等式，还可以依据这些基本算律经过恒等变形证明其他集合等式或包含关系。

例 3-7　利用集合演算证明下述等式。

(1) $A\bigcup(A\bigcap B)=A$。　　(2) $A\bigcap(B-C)=(A\bigcap B)-(A\bigcap C)$。

(3) $(B-A)\cup A=B\cup A$。　　(4) $\sim(A\cup(B\cap C))=(\sim B\cup\sim C)\cap\sim A$。

证明　(1) $A\cup(A\cap B)=(A\cap U)\cup(A\cap B)=A\cap(U\cup B)=A$。此为吸收律。

(2) $(A\cap B)-(A\cap C)=(A\cap B)\cap\sim(A\cap C)=(A\cap B)\cap(\sim A\cup\sim C)$

$=(A\cap B\cap\sim A)\cup(A\cap B\cap\sim C)=\varnothing\cup(A\cap(B\cap\sim C))$

$=A\cap(B-C)$。

(3) $(B-A)\cup A=(B\cap\sim A)\cup A=(B\cup A)\cap(\sim A\cup A)=(B\cup A)\cap U=B\cup A$。

(4) $\sim(A\cup(B\cap C))=\sim A\cap\sim(B\cap C)=\sim(B\cap C)\cap\sim A=(\sim B\cup\sim C)\cap\sim A$。

用恒等变形演算证明集合相等经常采取的方法是将复杂的表达式进行化简，但需要一定的技巧，应用范围也有限。

3.3.2　基于定义的集合运算证明方法

集合运算证明的核心问题是集合包含，即$\mathcal{A}\subseteq\mathcal{B}$，基于定义的证明方法就是：由$\forall x\in\mathcal{A}$的假定出发，推证出$x\in\mathcal{B}$的结论。

集合的名字可以变化，集合的元素可以变化，但由这种假定（前提）到结论的推证过程是确定的。

例 3-8　设$A\subseteq B$，求证$A\cap C\subseteq B\cap C$。

证明　这里的$\mathcal{A}=A\cap C$，$\mathcal{B}=B\cap C$。

对$\forall x$，若$x\in\mathcal{A}$，由集合交的定义，有

$$x\in A\wedge x\in C。$$

因为$A\subseteq B$，有

$$x\in B\wedge x\in C。$$

故$x\in\mathcal{B}$。结论成立。

[辨析] 观察要证明的结论，而不是条件！做出正确的假设“$\forall x\in\mathcal{A}$”并明确要推证的结论“$x\in\mathcal{B}$”之后，再细致研究题目给定的其他条件。

观察证明过程可知，集合的包含证明就是将结论中的集合“替代”定义中的集合，再逐个翻译、组合定义的过程。

$$\forall x,\ x\in\mathcal{A}\Leftrightarrow_{(A\cap C\text{定义})}x\in A\wedge x\in C\Rightarrow_{(A\subseteq B\text{定义})}x\in B\wedge x\in C\Leftrightarrow_{(B\cap C\text{定义})}x\in\mathcal{B}$$

$$\mathcal{A}\subseteq\mathcal{B}\text{定义}$$

例 3-9　证明$\sim(A\cup B)=\sim A\cap\sim B$。

证明　先推证$\sim(A\cup B)\subseteq\sim A\cap\sim B$。

对$\forall x$，有

$$\begin{aligned}x\in\sim(A\cup B)&\Rightarrow\neg\, x\in(A\cup B)\Rightarrow\neg(x\in A\vee x\in B)\\&\Rightarrow\neg\, x\in A\wedge\neg\, x\in B\Rightarrow x\in\sim A\wedge x\in\sim B\\&\Rightarrow x\in\sim A\cap\sim B。\end{aligned}$$

由于上述过程都是可逆的，有$\sim A\cap\sim B\subseteq\sim(A\cup B)$，结论成立。

例 3-10 证明 $A-B=A-(A\cap B)$。

证明 先推证 $A-B\subseteq A-(A\cap B)$。

对 $\forall x$，有

$$x\in A-B\Rightarrow x\in A\wedge x\notin B\Rightarrow x\in A\wedge x\notin A\cap B\Rightarrow x\in A-(A\cap B)。$$

再推证 $A-(A\cap B)\subseteq A-B$。

对 $\forall x$，有

$$\begin{aligned}x\in A-(A\cap B)&\Rightarrow x\in A\wedge\neg\, x\in A\cap B\Rightarrow x\in A\wedge\neg(x\in A\wedge x\in B)\\&\Rightarrow x\in A\wedge(\neg\, x\in A\vee\neg\, x\in B)\\&\Rightarrow(x\in A\wedge\neg\, x\in A)\vee(x\in A\wedge\neg\, x\in B)\\&\Rightarrow x\in A\wedge\neg\, x\in B\Rightarrow x\in A-B。\end{aligned}$$

结论成立。

例 3-11 证明 $A\oplus(B\oplus C)=(A\oplus B)\oplus C$，即对称差运算⊕满足结合律。

证明 对 $\forall x$，有

$$\begin{aligned}x\in A\oplus(B\oplus C)&\Rightarrow x\in A\,\overline{\vee}\,(x\in B\,\overline{\vee}\,x\in C)\\&\Rightarrow(x\in A\,\overline{\vee}\,x\in B)\,\overline{\vee}\,x\in C\Rightarrow x\in(A\oplus B)\oplus C。\end{aligned}$$

故 $A\oplus(B\oplus C)\subseteq(A\oplus B)\oplus C$。

因为上述蕴含关系都是可逆的，故 $(A\oplus B)\oplus C\subseteq A\oplus(B\oplus C)$。结论成立。

此例证明依赖于命题联结词 $\overline{\vee}$ 满足结合律的事实。

例 3-12 已知 $A\oplus B=A\oplus C$，问是否必有 $B=C$？

解 必有 $B=C$，这只要证明集合 B 和 C 相互包含，先推证 $B\subseteq C$。

对 $\forall x$，若 $x\in B$。分两种情况讨论：

(a) 若 $x\in A$，则 $x\notin A\oplus B$。因 $A\oplus B=A\oplus C$，有 $x\notin A\oplus C$。又因为 $x\in A$，必有 $x\in C$。

(b) 若 $x\notin A$，则 $x\in A\oplus B$。因 $A\oplus B=A\oplus C$，有 $x\in A\oplus C$。又因为 $x\notin A$，必有 $x\in C$。

总之，有 $x\in C$，即 $B\subseteq C$。

同理可证 $C\subseteq B$。结论成立。

此题目也可以采用集合算律来证明：

因 $A\oplus B=A\oplus C$，有

$$A\oplus(A\oplus B)=A\oplus(A\oplus C)。$$

由对称差运算⊕满足结合律，有

$$(A\oplus A)\oplus B=(A\oplus A)\oplus C。$$

因 $A\oplus A=\varnothing$，得 $\varnothing\oplus B=\varnothing\oplus C$，知 $B=C$。

[辨析] 给出一定的条件，要求说明某论断是否成立是常见的问题形式。若给出肯定回答，一般需要完成一次证明，而否定回答时可举出一个说明论断不真的例子（常称为“反例”）。

例 3-13 对于集合 A、B、C，问在什么条件下，下列命题为真？

(1) $(A-B)\cup(A-C)=A$。　　(2) $(A-B)\cup(A-C)=\varnothing$。

(3) $(A-B)\bigcap(A-C)=\varnothing$。　　(4) $(A-B)\oplus(A-C)=\varnothing$。

解　此类问题应尽量化简等式左边的表达式，以得到能够容易说明其实质的简单关系。

(1) 因为

$$(A-B)\bigcup(A-C)=(A\bigcap\sim B)\bigcup(A\bigcap\sim C)$$
$$=A\bigcap(\sim B\bigcup\sim C)=A\bigcap\sim(B\bigcap C)=A-(B\bigcap C)。$$

因此，结论成立的条件是 A 与 $B\bigcap C$ 不相交，即 $A\bigcap B\bigcap C=\varnothing$。

(2) 题目等同于 $A-(B\bigcap C)=\varnothing$，故结论成立的条件是 $A\subseteq B\bigcap C$。

(3) 因为

$$(A-B)\bigcap(A-C)=(A\bigcap\sim B)\bigcap(A\bigcap\sim C)$$
$$=A\bigcap(\sim B\bigcap\sim C)=A\bigcap\sim(B\bigcup C)=A-(B\bigcup C)。$$

因此，结论成立的条件是 $A\subseteq B\bigcup C$。

(4) 因为对于任何集合 X，只有 $X\oplus X=\varnothing$。因此，结论成立的条件是 $A-B=A-C$。

[延伸] 利用集合的基本运算可以衍生出两个著名的原理，即“容斥原理”（或称“包含排斥原理”，inclusion-exclusion principle）和“鸽巢原理”（pigeonhole principle），它们是被广泛应用的计数技术[2,3]。

容斥原理可描述为“合并后集合的元素个数等于各集合的元素个数之和除去其共同元素的个数”，而鸽巢原理可描述为“若 n 个集合中所包含元素个数的总和大于 n，则至少有一个集合包含 2 个或更多个元素”。

例如，若 A_1 和 A_2 为有限集合，我们不能直接用 $|A_1\bigcup A_2|=|A_1|+|A_2|$ 来计算 $A_1\bigcup A_2$ 的元素个数，除非 $A_1\bigcap A_2=\varnothing$。否则，$A_1\bigcap A_2$ 部分被重复地累加了一次。正确的做法是将重复累加的元素个数去除：

$$|A_1\bigcup A_2|=|A_1|+|A_2|-|A_1\bigcap A_2|。$$

这就是容斥原理，其含义是包含整体 $|A_1|+|A_2|$ 并排斥掉共同的部分 $|A_1\bigcap A_2|$。

在实际使用时，容斥原理有两种主要应用形式。若 A_1 和 A_2 为有限集合，则

(1) $|A_1\bigcup A_2|=|A_1|+|A_2|-|A_1\bigcap A_2|$。

(2) $|\sim(A_1\bigcup A_2)|=|\sim A_1\bigcap\sim A_2|=|U|-(|A_1|+|A_2|)+|A_1\bigcap A_2|$。

式(2)不过是计算式(1)中 $A_1\bigcup A_2$ 的余集的元素个数。

例如，计算以 1 开始或者以 00 结束的 8 位二进制符号串的个数。可记 A、B 分别是以 1 开始和以 00 结束的 8 位二进制符号串集合。注意到二进制串中的字符只有 0 和 1 两种状态，则 $|A|=2^7$，$|B|=2^6$。因为 $|A\bigcap B|=2^5$，故 $|A\bigcup B|=2^7+2^6-2^5=160$。

对含有 n 个有限集合 A_i 的一般情况，容斥原理的基本形式为：

$$|A_1\bigcup A_2\bigcup\cdots\bigcup A_n|=\sum_{1\leqslant i\leqslant n}|A_i|-\sum_{1\leqslant i<j\leqslant n}|A_i\bigcap A_j|+\sum_{1\leqslant i<j<k\leqslant n}|A_i\bigcap A_j\bigcap A_k|+\cdots+(-1)^{n-1}|A_1\bigcap A_2\bigcap\cdots\bigcap A_n|。$$

思考与练习 3.3

3-26 对任意集合 A、B、C，用运算定义验证下述性质。

(a) $(A\cap B)\cap C = A\cap(B\cap C)$。 (b) $(A\cup B)\cup C = A\cup(B\cup C)$。

(c) $A\cap(B\cup C) = (A\cap B)\cup(A\cap C)$。 (d) $A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$。

3-27 将 $?\cap(A\cup B) = A$ 和 $A\cup(A\cap B) = ?$ 中的“？”换成适当的集合使等式成立。它们是什么算律？

3-28 给出集合表达式 $(A-C)\cup B = A\cup B$ 成立的充分必要条件。

3-29 设 A、B 为集合，证明：

(a) $A\oplus B = B\oplus A$。 (b) $(A\oplus B)\oplus B = A$。

3-30 设 A、B 为集合，并分别满足下述条件，问集合 A 与 B 各是什么关系？

(a) $A-B = B$。 (b) $A-B = B-A$。

(c) $A\cap B = A\cup B$。 (d) $A\oplus B = A$。

3-31 设 A、B 为集合，证明 $A\subseteq B$ 当且仅当 $\sim B\subseteq\sim A$。

3-32 设 A、B、C 为集合，证明：

(a) $(A-B)-C = (A-C)-B$。 (b) $A-(B\cup C) = (A-B)-C$。

(c) $(A-C)-(B-C) = (A-B)-C$。

3-33 对于集合 A、B、C，判断下列命题是否为真并予以说明。

(a) $A\cap(B\oplus C) = (A\cap B)\oplus(A\cap C)$。 (b) $A\cup(B\oplus C) = (A\cup B)\oplus(A\cup C)$。

3-34 说明下列命题是否正确并说明理由。

(a) $A-(B\cup C) = (A-B)\cup C$。 (b) $(A-B)\cap(B-A) = \varnothing$。

(c) $(A\cap B)\cup(B-A) = B$。

3-35 设 A、B 为集合，下述各式中哪个命题与 $A\subseteq B$ 不等价？

(a) $A\oplus B\subseteq B$。 (b) $A\cup B = B$。

(c) $A\cap B = B$。 (d) $\mathscr{P}(A)\subseteq\mathscr{P}(B)$。

3-36 在 10 名学生中选修 Android 编程的有 5 人，选修 IOS 编程的有 7 人，同时选修 Android 编程和 IOS 编程的有 3 人。问 Android 编程和 IOS 编程都没选修的学生有几人？

3-37 求由 a、b、c、d 四个字母构成的 n 位符号串中，a、b 和 c 至少出现一次的符号串数目。

3.4 序偶与笛卡儿积

集合既可以由简单元素构成，也可由复杂元素如集合构成。特别地，当集合元素是一类特殊的集合——序偶时有着特殊的作用，这样的集合是构成关系和函数的基础。

3.4.1　序偶与元组

[定义 3-14] 序偶（ordered pairs）是两个元素组成的有序集合，记作$<x,y>$，也称为**有序对**或**二元组**。x、y 分别称为序偶的第一、第二个元素。

序偶一词本身的含义就是“有序的对”。

生活中的许多事物之间有一定关系，且成对出现，如平面上点的 2 个坐标、飞机票与座位、上与下、左与右及计算机上的网线接头与插口等。计算机内可以用<地址码，操作码>来构成单地址指令，手机电话簿中常用<拼音，人名>方式作为索引。

[辨析] 因为强调次序的原因，若$x \neq y$，则$<x,y> \neq <y,x>$。注意序偶的限界符既不是“{ }”，也不是“( )”，而是“< >”。通常$\{x,y\}$表示一般集合，(x,y)表示 2 个元素组成的无序集合。

[定义 3-15]　两个序偶相等，即$<x,y>=<a,b>$当且仅当$x=a$且$y=b$。

例 3-14　若已知$<2x+2,y>=<2y,x-y>$，求 x 和 y。

解　由定义，可构成一个二元一次方程组

$$2x+2=2y,\quad y=x-y。$$

解之得$x=-2$，$y=-1$。

上述定义可推广到 ***n* 元组**，如三元组、四元组等，形式为$<x_1,x_2,...,x_n>$，其含义是：

$$<x_1,x_2,...,x_n>=<<x_1,x_2,\cdots,x_{n-1}>,x_n>。$$

一般情况下，$<x_1,x_2,\cdots,x_n> \neq <x_1,<x_2,\cdots,x_n>>$。

[辨析] 严格讲，$<x_1,<x_2,\cdots,x_n>>$不是一个 n 元组，而是二元组。该二元组由一个简单元素 x_1 和一个 $n-1$ 元组$<x_2,\cdots,x_n>$组成。

在最初的计算机设计中，一个字节并不是固定的 8 个二进制位。因此，早期的国际标准中为了防止歧义，常称一个 8 位二进制串为八元组而不是字节。一个关系数据库是由若干张二维表组成的，每个表又由若干记录组成，而每个记录都是一个 n 元组。

[延伸] 实际上，程序设计中的所有运算和含有参数的函数在本质上都是以一个多元组为参数的。例如，对于如下的 C 语言函数 f：

```
void  f(int  x, double  y, char  z);
```

它的调用形式为 f(2, 3.5, ‘a’)，这里的参数数量、类型和次序都是不可改变的，故是一个三元组，只是没有（也不需要）写成<2,3.5, ‘a’>的形式而已[1]。

3.4.2　笛卡儿积

由于序偶的两个元素各来自于一个集合，因此，任给两个集合 A 和 B，都可以构造一种序偶的集合。

[定义 3-16]　若 A、B 是集合，它们构成的**笛卡儿积**是一个序偶集合，序偶的第一元素取自于 A，而第二个元素取自于 B，记作 $A\times B$，即

$$A\times B=\{<x,y>|x\in A\wedge y\in B\}。$$

笛卡儿积也称为集合的**直（接）积**，或者**叉乘**。这是一个核心性的定义。

[理解] 若 $<x,y>\in A\times B$，必有结论 $x\in A$ 且 $y\in B$。反之，对 $\forall x\in A$，$\forall y\in B$，必有结论 $<x,y>\in A\times B$。由于集合 A 和 B 可以相同，因此，$\forall x\in A$，必有结论 $<x,x>\in A\times A$。

例 3-15 设 $A=\{a,b\}$，$B=\{1,2,3\}$，求 $A\times B$ 和 $B\times A$。

解

$$A\times B=\{<a,1>,<a,2>,<a,3>,<b,1>,<b,2>,<b,3>\},$$

$$B\times A=\{<1,a>,<1,b>,<2,a>,<2,b>,<3,a>,<3,b>\}。$$

在组成笛卡儿积时，要求来自 A、B 的元素是全部的，因此，集合中不能缺少任何一个序偶。同时，对于有限的笛卡儿积，显然有 $|A\times B|=|A|\times|B|$。

事实上，如果 $A=B=\mathbf{R}$，笛卡儿积 $\mathbf{R}\times\mathbf{R}$ 就是平面直角坐标系。可见，一般的笛卡儿积等同于“离散的直角坐标系”。

与简单集合类似，笛卡儿积部分的主要问题还是证明集合包含。不过，笛卡儿积的元素是序偶，因此，证明 $A\times B\subseteq C\times D$ 仍是从定义出发，形式为：

$\forall <x,y>\in A\times B\Rightarrow x\in A\wedge y\in B\Rightarrow$ 其他定义和条件的应用 $\Rightarrow <x,y>\in C\times D$。

很容易得出以下结论，这是笛卡儿积的常用性质。

[定理 3-5] 对于任意集合 A、B 和 C，有

(1) $A\times\varnothing=\varnothing\times A=\varnothing$。

(2) 通常，笛卡儿积不满足交换律，即

$$A\times B\neq B\times A。$$

(3) 笛卡儿积不满足结合律，即

$$(A\times B)\times C\neq A\times(B\times C)。$$

其实，前者是三元组集合，而后者仅是二元组集合。

为了与 n 元组的含义一致，约定：

$$A_1\times A_2\times\cdots\times A_n=(A_1\times A_2\times\cdots\times A_{n-1})\times A_n。$$

特别地，$A^n=\underbrace{A\times A\times\cdots\times A}_{n个}$，$n\geqslant 1$。

(4) 笛卡儿积对交和并运算满足分配律，即

① $A\times(B\cup C)=(A\times B)\cup(A\times C)$；　② $(B\cup C)\times A=(B\times A)\cup(C\times A)$；

③ $A\times(B\cap C)=(A\times B)\cap(A\times C)$；　④ $(B\cap C)\times A=(B\times A)\cap(C\times A)$。

证明 这里仅证明①，其余性质的证明方法类似。

对 $\forall <x,y>$，有

$<x,y>\in A\times(B\cup C)$　　注：来自集合包含的假定

$\Leftrightarrow_{(笛卡儿积定义)} x\in A\wedge y\in B\cup C$

$\Leftrightarrow_{(集合并定义)} x\in A\wedge(y\in B\vee y\in C)$

$\Leftrightarrow_{(命题分配律)}(x\in A\wedge y\in B)\vee(x\in A\wedge y\in C)$

$\Leftrightarrow_{(笛卡儿积定义)}(<x,y>\in A\times B\vee(<x,y>\in A\times C)$

$\Leftrightarrow_{(集合并定义)}<x,y>\in(A\times B)\bigcup(A\times C)$。

故结论成立。

例 3-16　求证：

(1) 若 A、B、C、D 非空，则 $A\subseteq C$ 且 $B\subseteq D\Leftrightarrow A\times B\subseteq C\times D$。

(2) 若 $C\neq\varnothing$，则 $A\subseteq B\Leftrightarrow A\times C\subseteq B\times C\Leftrightarrow C\times A\subseteq C\times B$。

证明　(1) ①　$A\subseteq C\wedge B\subseteq D\vdash A\times B\subseteq C\times D$。

对$\forall<x,y>$，有

$$<x,y>\in A\times B\Rightarrow x\in A\wedge y\in B\Rightarrow x\in C\wedge y\in D\Rightarrow<x,y>\in C\times D。$$

故 $A\times B\subseteq C\times D$。

②　$A\times B\subseteq C\times D\vdash A\subseteq C\wedge B\subseteq D$。

对$\forall x\in A$ 和$\forall y\in B$，有$<x,y>\in A\times B$。因为 $A\times B\subseteq C\times D$，有$<x,y>\in C\times D$，故 $x\in C$ 且 $y\in D$，即 $A\subseteq C$ 且 $B\subseteq D$。结论成立。

(2) 先说明 $A\subseteq B\Leftrightarrow A\times C\subseteq B\times C$。

①　$A\subseteq B\vdash A\times C\subseteq B\times C$。

对 $\forall<x,y>$，有

$$<x,y>\in A\times C\Rightarrow x\in A\wedge y\in C\Rightarrow x\in B\wedge y\in C\Rightarrow<x,y>\in B\times C。$$

②　$A\times C\subseteq B\times C\vdash A\subseteq B$。

对$\forall x\in A$，因为 $C\neq\varnothing$，故 $\exists y(y\in C)$ 成立。于是，有

$$<x,y>\in A\times C。$$

因此，$<x,y>\in B\times C$，得 $x\in B$，即 $A\subseteq B$。结论成立。

同理可证，$A\subseteq B\Leftrightarrow C\times A\subseteq C\times B$。可见三者均等价。

[辨析] 这里的 $C\neq\varnothing$ 很重要，它保证了 C 至少含有一个以上的元素，从而与 A 中的元素构成序偶。

例 3-17　对任意集合 A、B、C、D，判断下述命题是否成立。

(1)　$A\times B=A\times C\Rightarrow B=C$。　　(2)　$A-(B\times C)=(A-B)\times(A-C)$。

(3) 存在集合 A，使得 $A\subseteq A\times A$。

解　(1) $A=\varnothing$ 时不成立，否则成立。

(2) 除非 A、B、C 均为空集，否则不成立。

(3) 成立，如取 $A=\varnothing$。事实上，$\varnothing$ 是使命题成立的唯一一个集合。

例 3-18　证明：若 $X\times X=Y\times Y$，则 $X=Y$。

证明　先推证 $X\subseteq Y$。对$\forall x$，有

$$x\in X\Rightarrow<x,x>\in X\times X\Rightarrow<x,x>\in Y\times Y\Rightarrow x\in Y。$$

同理可证 $Y \subseteq X$ 。结论成立。

[理解] 题目要证明的是 $X \subseteq Y$ 且 $Y \subseteq X$ ，而不是 $X \times X \subseteq \cdots$ ，不能从 $\forall < x,y > \in X \times X$ 的假定出发，更不能用 $\forall < x,x > \in X \times X$ 作为前提进行论证。

思考与练习 3.4

3-38 对于集合 A、B，如果 $a \in A$ 且 $b \in B$，一定有 $< a,b > \in A \times B$ 吗？一定有 $< a,a > \in A \times A$ 吗？

3-39 设 A 为集合， A^n 的含义是什么？可以采用这种记法的原因是什么？

3-40 若 $A = \{0,1\}$， $B = \{1,2\}$，计算下述集合。

(a) $A \times \{1\} \times B$ 。 (b) $A^2 \times B$ 。

(c) $(B \times A)^2$ 。

3-41 设 $A = \{\varnothing, \{\varnothing\}\}$，求 $\mathscr{P}(A) \times A$ 。

3-42 若题目要证明的结论为 $X \times X \subseteq Y \times Y$ 。如下的证明方法正确吗？

$\forall < x,x > \in X \times X$ ，因为……，所以， $< x,x > \in Y \times Y$ 。故 $X \times X \subseteq Y \times Y$ 。

3-43 判断下述命题是否成立并说明理由。

(a) $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times D)$ 。 (b) $(A - B) \times (C - D) = (A \times C) - (B \times D)$ 。

(c) $(A \oplus B) \times (C \oplus D) = (A \times C) \oplus (B \times D)$ 。 (d) $(A - B) \times C = (A \times C) - (B \times C)$ 。

(e) $(A \oplus B) \times C = (A \times C) \oplus (B \times C)$ 。

3-44 若 $S \times A = S \times B$ ，问是否有 $A = B$ ？说明使结论成立应增加的条件并证明。

第 4 章　关　　系

关系（relation）是一个基本概念，最简单的关系体现了两个事物之间的联系，如数的大于关系、师生关系、上下级关系、元素与集合的属于关系、集合的包含关系、命题的蕴含关系和等价关系、机票与座位的对应关系以及两个人是否相识、同属一个小组或血缘等。很明显，这样的关系可用序偶来表示。多个对象之间也存在类似的多元关系，此时可用 n 元组来表示。计算机科学中，建立在关系理论基础上的数据库称为关系型数据库。

这里仅讨论二元关系。

4.1　二元关系的含义与表示

4.1.1　二元关系

[定义 4-1] 任意的序偶集合称为一个**二元关系**（binary relation）。若 R 是二元关系，且序偶 $<x,y>\in R$，可记作 xRy，称 x 与 y **有关系** R。若序偶 $<x,y>\notin R$，可记作 $x\not R y$，称 x 与 y **没有关系** R。

例如，$R=\{<1,a>,<2,c>\}$是一个二元关系，实数集上的大于等于关系“≥”可记作

$$\geqslant=\{<x,y>|x\in\mathbf{R}，且\ y\in\mathbf{R}，且\ x\ 大于或等于\ y\}。$$

[辨析] 用 R 表示关系源自单词 relation 的第一个字母，生活中最常用的关系不用字母而是用其他符号表示，如>、<、=、≥、≤、≠、∈等，且 xRy 的表示形式比 $<x, y>\in R$ 更常见。例如，虽然 $2\leqslant 5$ 和 $X\subseteq Y$ 也可写成 $<2, 5>\in\leqslant$ 和 $<X, Y>\in\subseteq$，但后者十分罕见。不等于关系、不属于关系中的序偶表示为 $3\neq 7$ 和 $2.5\notin\mathbf{N}$，而不是 $<3, 7>\in\neq$ 和 $<2.5, \mathbf{N}>\in\notin$。

若 R 为二元关系，由 $<x, y>\in R$ 的所有 x 组成的集合 dom R 称为 R 的**前域**，即

$$\text{dom}\ R=\{x|\exists y(<x, y>\in R)\}。$$

由 $<x, y>\in R$ 的所有 y 组成的集合 ran R 称为 R 的**值域**，即

$$\text{ran}\ R=\{y|\exists x(<x, y>\in R)\}。$$

直接说明关系的前域和值域可以更清楚地描述一个关系，且称 FLD R = dom $R\bigcup$ ran R 为 R 的域。

[定义 4-2] 设 X 和 Y 为集合，笛卡儿积 $X\times Y$ 的任意子集 R 称为 X **到** Y **的（二元）关系**。若 $X=Y$，则称 R 为 X **上的二元关系**。

例如，$A=\{1,2,3,4\}$，≤为 A 上的“小于或等于”关系，即

$$\leqslant=\{<x, y>|\ x, y\in A\wedge x\ 小于或等于\ y\}。$$

那么，有

$\leqslant$={<1,1>,<1,2>,<1,3>,<1,4>,<2,2>,<2,3>,<2,4>,<3,3>,<3,4>,<4,4>}。

又如，*Code*={20150101, 20150102, 20150103}表示学号集合，*Name*={马云，李彦宏，雷军}表示学生姓名集合，则 *R* = {<20150101,马云>, <20150102,李彦宏>, <20150103, 雷军>}是 *Code*×*Name* 的子集，构成 *Code* 到 *Name* 的一个二元关系。它是关系型数据库中的一张表。

表 4-1

学号	姓名
20150101	马云
20150102	李彦宏
20150103	雷军

Code 和 *Name* 分别是关系的前域和值域。

对于有限集合 X 和 Y，若 $|X|=n$，$|Y|=m$，则 $|X\times Y|=mn$，因为所有 X 到 Y 的二元关系都是 $X\times Y$ 的子集，故 X 到 Y 的所有二元关系构成集合 $\mathscr{P}(X\times Y)$，这说明，共有 2^{mn} 个 X 到 Y 的二元关系。特别地，X 上的二元关系有 2^{n^2} 个。其中，$\varnothing$ 称为 X 上（或 X 到 X）的“空关系”，而 $X\times X$ 称为 X 上（或 X 到 X）的“全关系”。

例 4-1 设 $A=\{a,b\}$，试求出 $\mathscr{P}(A)$上的包含关系$\subseteq$。

解 因为 $\mathscr{P}(A)=\{\varnothing, \{a\}, \{b\}, A\}$，有

$\subseteq$= {<Ø,Ø>,<Ø,{a}>,<Ø,{b}>,<Ø,A>,<{a},{a}>,<{a},A>,<{b},{b}>,<{b},A>,<A,A>}。

例 4-2 对于任意集合 $A\subseteq \mathbf{Z}^+$，A 上的整除关系是一种常用的关系。通常，x 能整除 y 记作“$x\,|\,y$”，则 A 上的整除关系定义为

$$R=\{<x,y>\,|\,x,y\in A\wedge x\,|\,y\}。$$

求 $A=\{1,2,3,4,6\}$上的整除关系。

解 A 上的整除关系为

R={<1,1>,<2,2>,<3,3>,<4,4>,<6,6>,<1,2>,<1,3>,<1,4>,<1,6>,<2,4>,<2,6>,<3,6>}。

一般可直接用符号“|”表示整除关系。

在 X 上的二元关系中，恒等关系是一个比较特殊且重要的关系。

[定义 4-3] $I_X=\{<x,x>\,|\,x\in X\}$ 称为 X 上的**恒等关系**。

例如，$X=\{1,2,3\}$，则 I_X = {<1,1>,<2,2>,<3,3>}。

[辨析] 关系 I_X就是由所有 X 的元素 x 与自身组成的序偶的集合。如果少了或多了其他序偶，就不再是恒等关系。例如，$X=\{1,2\}$，则{<1,1>}和{<1,1>,<2,2>,<1,2>}都不是恒等关系。

[理解] 若 $x\in X$，必有结论 $<x,x>\in I_X$；若 $<x,y>\in I_X$，必有结论 $x=y$。

因为关系是集合，如果两个二元关系 *R* 和 *S* 定义在同样的域上，则可进行集合的交、并、补等运算，其结果也是一个二元关系。

例 4-3 设 $X=\{1,2,3,4\}$，有 X 上的二元关系 $H=\{<x,y>|(x-y)/2$ 是整数$\}$，$S=\{<x,y>|(x-y)/3$ 是正整数$\}$，求 $H\cup S$、$H\cap S$、$S-H$ 和 $\sim H$。

解 因为

$$H=\{<1,1>,<2,2>,<3,3>,<4,4>,<2,4>,<4,2>,<3,1>,<1,3>\},\quad S=\{<4,1>\}。$$

由此可计算出：

$$H \cup S = \{<1,1>,<2,2>,<3,3>,<4,4>,<2,4>,<4,2>,<3,1>,<1,3>,<4,1>\},$$
$$H \cap S = \varnothing,$$
$$S - H = \{<4,1>\},$$
$$\sim H = X \times X - H = \{<1,2>,<2,1>,<1,4>,<4,1>,<2,3>,<3,2>,<3,4>,<4,3>\}。$$

H 代表了一类非常重要的关系，其含义是 x 与 y 有关系 H，当且仅当 x 与 y 除以 2 的余数相同，称为“模 2 同余关系”。一般地，对于一个不小于 2 的整数 m，可定义“模 m 同余关系”为 $H = \{<x, y> | (x-y)/m$ 是整数$\}$。为了简单，通常用 $x \equiv y(\mathrm{mod}\, m)$ 表示“x 与 y 除以 m 的余数相同”，则 $\mathbf{Z}$ 模 m 同余关系可记为：

$$H = \{<x, y> | x, y \in \mathbf{Z} \wedge x \equiv y(\mathrm{mod}\, m)\}。$$

4.1.2　关系的矩阵和图表示法

除了集合表示法之外，有限集合上的二元关系还可以采用关系矩阵或关系图来表示。

1．关系矩阵

[定义 4-4] 设 $X = \{x_1, x_2, \cdots, x_m\}$，$Y = \{y_1, y_2, \cdots, y_n\}$，$R$ 是 X 到 Y 的关系。定义 R 的**关系矩阵**（matrix of relation）为 $M_R = [r_{ij}]_{m \times n}$，其中，

$$r_{ij} = \begin{cases} 1 & , < x_i, y_j > \in R \\ 0 & , < x_i, y_j > \notin R \end{cases}, \quad 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n。$$

例如，设 $A = \{1,2,3,4\}$，则 A 上的大于关系>={<2,1>,<3,1>,<3,2>,<4,1>,<4,2>,<4,3>}，其关系矩阵为

$$M_{>} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}。$$

2．关系图

利用结点加连线方式可以构成更直观的关系图 G_R（graph of relation），具体方法为：

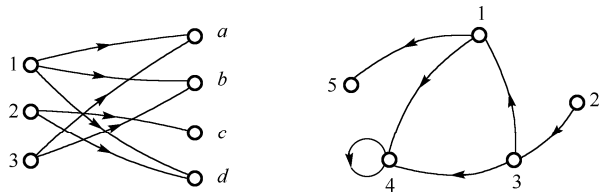
① 用圆圈表示集合元素，称为“结点”；

② 若$<x, y> \in R$，则有一条由 x 到 y 的带箭头的连线，称为“边”或“弧”。

关系图就是常见的有向图。

在前域 X 与值域 Y 不同时，要标记出这两个集合的元素。例如，$A = \{1,2,3\}$，$B = \{a,b,c,d\}$，A 到 B 的关系 $R = \{<1,a>,<1,b>,<1,d>,<2,c>,<2,d>,<3,a>,<3,b>\}$的关系图为图 4-1(a)。

对于定义在集合 X 上的二元关系，其关系图一般只标记出一组集合的元素。设 $A = \{1,2,3,4,5\}$，在 A 上的二元关系 $R = \{<1,5>,<1,4>,<2,3>,<3,1>,<3,4>,<4,4>\}$的关系图为图 4-1(b)。



(a) (b)

图 4-1

图中的圆圈大小和位置、线段长短和曲直都无关紧要，但连线的有无和方向必须正确。类似结点 4 上由自身到自身的连线称为“自回路”或“环”。

[延伸] “社会网络分析（SNA）”是一种针对不同社会行动者构成的网络结构的社会关系与结构进行分析的方法，大数据技术的兴起进一步推动了社会网络分析在职业流动、城市化、世界政治和经济体系、国际贸易等领域的应用，并发挥了重要作用。关系是该领域中的研究对象并得到了更充分的扩展。它不仅研究了两个行动者之间的关系，还通过连接度等因素将整个对象集划分为组、子群和群等部分对象集，从而发现它们之间的联系和运作规律。参见 http://wiki.mbalib.com/wiki/社会网络分析。

思考与练习 4.1

4-1 二元关系、X 到 Y 的关系及 X 上的关系各是什么含义？

4-2 设 $A=\{0,1,2,3,4\}$，定义 A 上的关系 $R=\{<x,y>\mid x=y+1 \text{或} y=x/2\}$，试用列举法写出关系 R。

4-3 设 $A=\{a,b,c,d\}$，定义 A 上的二元关系 $R=\{<a,b>,<b,d>,<c,c>\}$，$S=\{<a,c>,<b,d>,<d,b>\}$，求 $R\cap S$、$R\cup S$、$R-S$、$R\oplus S$ 和 $\sim R$。

4-4 有如下的二元关系 R，用列举法写出这些关系，求出 dom R、ran R，计算它们的关系矩阵并画出关系图。

(a) $A=\{0,1,2,3,4,5,6\}$，$R=\{<x,y>\mid x\geqslant 2 \text{且} x\mid y\}$。

(b) $A=\{0,1,2,3,4,5\}$，$R=\{<x,y>\mid 1\leqslant x-y\leqslant 2\}$。

(c) $A=\{2,3,4,5,6\}$，$R=\{<x,y>\mid x \text{与} y \text{互素}\}$，$x$ 与 y 互素意指 x 与 y 的最大公约数为 1。

4-5 对于集合 A，如果 $<x,y>\in I_A$，能得到什么结论？

4-6 若 $X=\{0,1,2,3,4\}$，写出 I_X 的关系矩阵，画出其关系图。

4.2 关 系 运 算

这里介绍两种专门针对二元关系的运算。

4.2.1　关系求逆与复合

1．关系的逆

[定义 4-5] 设 R 是 X 到 Y 的二元关系，将其每个序偶的元素交换顺序所得到的关系称为 R 的**逆关系**，记作 R^{-1}（或 R^C）。符号表示为：

$$R^{-1}=\{<y,x>\mid <x,y>\in R\}。$$

[理解] 只要 $<x,y>\in R$，则 $<y,x>\in R^{-1}$；只要 $<y,x>\in R^{-1}$，则 $<x,y>\in R$。

例如，大于等于关系“≥”的逆就是小于等于关系“≤”。集合 $X=\{1,2,3\}$ 上的二元关系 $R=\{<1,1>,<2,2>,<3,3>,<1,2>,<2,3>\}$ 的逆 $R^{-1}=\{<1,1>,<2,2>,<3,3>,<2,1>,<3,2>\}$。

[定理 4-1] 设 R 是任意关系，则

(1) $(R^{-1})^{-1}=R$。　　(2) $\mathrm{dom}\,R^{-1}=\mathrm{ran}\,R$，$\mathrm{ran}\,R^{-1}=\mathrm{dom}\,R$。

由于关系本身是集合，因此，关系等式的证明仍是采用集合包含的定义。

证明　这里仅略证(1)，就是说明 $(R^{-1})^{-1}$ 与 R 互相包含。

对 $\forall <x,y>$，有

$$<x,y>\in (R^{-1})^{-1}\Leftrightarrow <y,x>\in R^{-1}\Leftrightarrow <x,y>\in R。$$

可见结论成立。

2．关系的复合

[定义 4-6] 设 R 和 S 分别是 X 到 Y 和 Y 到 Z 的关系，则 $R\circ S$ 称为 R 和 S 的**复合关系**（**合成关系**）。符号表示为

$$R\circ S=\{<x,z>\mid x\in X\wedge z\in Z\wedge \exists y(y\in Y\wedge <x,y>\in R\wedge <y,z>\in S)\}。$$

例 4-4　设 $A=\{2,3,6\}$，A 上的二元关系 $R=\{<3,3>,<3,2>,<6,2>\}$，$S=\{<3,1>,<2,2>,<2,3>\}$，求 $R\circ S$ 和 $S\circ R$。

解　$R\circ S=\{<3,1>,<3,2>,<3,3>,<6,2>,<6,3>\}$，$S\circ R=\{<2,3>,<2,2>\}$。

[辨析] 本质上，在计算复合关系时，R 与 S 可以是任何关系，也不必要求 R 的值域等于 S 的前域。R 与 S 的复合指将所有 R 与 S 中的序偶连接后形成的新序偶的集合。两个序偶<x,y>和<y,z>能连接的条件是前一序偶的第二元素与后一序偶的第一元素相同（都是 y）。

[理解] 若<x,y>∈R，<y,z>∈S，必有<x,z>∈$R\circ S$；若<a,b>∈$R\circ S$，必有 $t\in Y$，使得<a,t>∈R，<t,b>∈S。这里的 x、y、a 和 b 都可以相同或不同。

例 4-5　设 S、T 是集合 **N** 上的关系，定义为：

$$S=\{<x,y>\mid x,y\in \mathbf{N}\wedge y=x^3\},$$
$$T=\{<x,y>\mid x,y\in \mathbf{N}\wedge y=x+1\}。$$

求 S^{-1}、$S\circ T$ 和 $T\circ S$。

解 $S^{-1}=\{<y,x>|x,y\in\mathbf{N}\wedge y=x^3\}$。

计算复合关系时将 T 换一下符号会更清楚：

$$T=\{<y,z>|y,z\in\mathbf{N}\wedge z=y+1\}。$$

可见，S 与 T 中的序偶连接条件是 $z=y+1=x^3+1$，有 $S\circ T=\{<x,z>|x,z\in\mathbf{N}\wedge z=x^3+1\}$。

同理，$T\circ S=\{<x,y>|x,y\in\mathbf{N}\wedge y=(x+1)^3\}$。

[辨析] 如果视 S 为函数 $<x,y=f(x)>$，视 T 为函数 $<y,z=g(y)>$，则 $S\circ T$ 为两函数复合的结果 $<x,z=g(f(x))>$。

4.2.2 关系运算的性质

由于关系运算主要依据序偶元素的反序和合取联结词定义，它们也表现出一定的简单规律。更重要的是通过验证这些性质可以了解关系运算中体现的集合包含的证明方法。

[定理 4-2] 设 R、S、T 是任意关系，则

(1) $(R\circ S)\circ T=R\circ(S\circ T)$，即复合运算满足结合律。

(2) $(R\circ S)^{-1}=S^{-1}\circ R^{-1}$。

证明略。

[定理 4-3] 设 R 是 A 上的关系，则 $R\circ I_A=I_A\circ R=R$。

证明 仅证明 $R\circ I_A=R$，方法仍是集合的互相包含。

先推证 $R\circ I_A\subseteq R$。对 $\forall<x,y>$，有

$$\begin{aligned}&<x,y>\in R\circ I_A\\ &\Rightarrow_{(\text{复合关系定义})}\exists t(t\in A\wedge<x,t>\in R\wedge<t,y>\in I_A)\\ &\Rightarrow_{(I_A\text{定义})}\exists t(t\in A\wedge<x,t>\in R\wedge t=y)\\ &\Rightarrow<x,y>\in R。\end{aligned}$$

再推证 $R\subseteq R\circ I_A$。

对 $\forall<x,y>\in R$，因为 $<y,y>\in I_A$，有 $<x,y>\in R\circ I_A$。结论成立。

[定理 4-4] 设 R、S、T 是任意关系，则复合运算对交、并满足分配律：

(1) $R\circ(S\cup T)=(R\circ S)\cup(R\circ T)$；　　(2) $(S\cup T)\circ R=(S\circ R)\cup(T\circ R)$；

(3) $R\circ(S\cap T)=(R\circ S)\cap(R\circ T)$；　　(4) $(S\cap T)\circ R=(S\circ R)\cap(T\circ R)$。

证明 仅验证(1)。为叙述简单，设 R、S、T 都是定义在 X 上的二元关系。

先推证 $R\circ(S\cup T)\subseteq(R\circ S)\cup(R\circ T)$。对 $\forall<x,y>$，有

$$\begin{aligned}&<x,y>\in R\circ(S\cup T)\\ &\Rightarrow_{(\text{复合关系定义})}\exists t(t\in X\wedge<x,t>\in R\wedge<t,y>\in S\cup T)\\ &\Rightarrow_{(\text{集合并定义})}\exists t(t\in X\wedge<x,t>\in R\wedge(<t,y>\in S\vee<t,y>\in T))\\ &\Rightarrow_{(\text{命题分配律})}\exists t(t\in X\wedge((<x,t>\in R\wedge<t,y>\in S)\vee(<x,t>\in R\wedge<t,y>\in T)))\\ &\Rightarrow_{(\text{复合关系定义})}<x,y>\in R\circ S\vee<x,y>\in R\circ T\end{aligned}$$

$\Rightarrow_{(集合并定义)} < x,y > \in (R \circ S) \bigcup (R \circ T)$ 。

注意到上述蕴含关系都是等价的，反方向的蕴含关系也成立。故结论成立。

[定理 4-5] 设 R、S 是 A 到 B 的关系，则

(1) $(R \bigcup S)^{-1} = R^{-1} \bigcup S^{-1}$ 。

(2) $(R \bigcap S)^{-1} = R^{-1} \bigcap S^{-1}$ 。

(3) $(A \times B)^{-1} = B \times A$ 。

(4) $(\sim R)^{-1} = \sim (R^{-1})$，其中的 $\sim R = A \times B - R$ 。

(5) $(R - S)^{-1} = R^{-1} - S^{-1}$ 。

证明　仅证(5)。对 $\forall < x,y >$，有

$$\begin{aligned} < x,y > \in (R-S)^{-1} &\Leftrightarrow < y,x > \in R-S \\ &\Leftrightarrow < y,x > \in R \wedge < y,x > \notin S \\ &\Leftrightarrow < x,y > \in R^{-1} \wedge < x,y > \notin S^{-1} \\ &\Leftrightarrow < x,y > \in R^{-1} - S^{-1} 。 \end{aligned}$$

结论成立。

例 4-6　令 S 和 T 分别为 X 到 Y、Y 到 Z 的关系。对于 $A \subseteq X$，定义 $S(A) = \{y \mid < x,y > \in S \wedge x \in A\}$ 。证明：

(1) $S(A) \subseteq Y$ 。　　(2) $(S \circ T)(A) = T(S(A))$ 。

(3) $S(A \bigcup B) = S(A) \bigcup S(B)$ 。　　(4) $S(A \bigcap B) \subseteq S(A) \bigcap S(B)$ 。

[辨析] 分析此题目的目的是学会理解定义，并体会如何依据定义进行推理。

证明　根据 S 的定义，$S(A)$是在关系 S 之下，与 A 中元素构成序偶的 y 的集合，它被称为 S 在 A 上的限制。这里仅说明(2)。模仿 $S(A)$的定义可知：

$$(S \circ T)(A) = \{z \mid < x,z > \in (S \circ T) \wedge x \in A\},$$
$$T(S(A)) = \{z \mid < y,z > \in T \wedge y \in S(A)\}。$$

参见图 4-2。

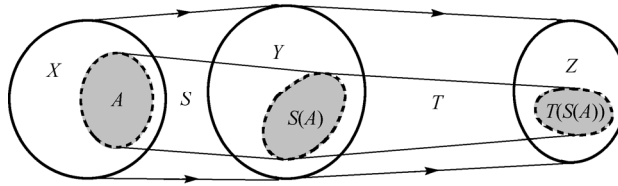


图 4-2

首先推证 $(S \circ T)(A) \subseteq T(S(A))$ 。对 $\forall z$，有

$$\begin{aligned} z \in (S \circ T)(A) &\Rightarrow \exists x(x \in A \wedge < x,z > \in S \circ T) \\ &\Rightarrow \exists x(x \in A \wedge \exists y(y \in Y \wedge < x,y > \in S \wedge < y,z > \in T)) \\ &\Rightarrow \exists x \exists y(x \in A \wedge y \in Y \wedge < x,y > \in S \wedge < y,z > \in T) \end{aligned}$$

$$\Rightarrow \exists y(\exists x(x \in A \wedge y \in Y \wedge < x, y > \in S) \wedge < y, z > \in T)$$
$$\Rightarrow \exists y(y \in S(A) \wedge < y, z > \in T)$$
$$\Rightarrow z \in T(S(A))。$$

上述命题间的蕴含实质是等价的，即相反方向的蕴含关系也真。结论成立。

4.2.3 利用关系图与关系矩阵实现关系运算

1. 由关系图实现关系运算

利用关系图很容易得到关系的逆和复合，其中，逆关系的关系图是通过将原关系图中的所有连线箭头方向取反得到的，而计算复合关系要将所有的两条“首尾相连”的连线组成一条连线。

例 4-7 设 $X=\{1,2,3,4\}$，$Y=\{2,3,4\}$，$Z=\{1,2,3\}$，S 和 T 分别是集合 X 到 Y 和 Y 到 Z 的关系，有

$$S=\{< x, y > \mid x \in X \wedge y \in Y \wedge x+y=6\}，$$
$$T=\{< y, z > \mid y \in Y \wedge z \in Z \wedge y-z=1\}。$$

求出 S 与 T 的复合关系 $S \circ T$，并绘制出 $S \circ T$ 的关系图。若 S 和 T 都是集合 X 上的关系，重新绘制出 $S \circ T$ 的关系图。

解 由条件得，$S=\{<2,4>,<3,3>,<4,2>\}$，$T=\{<2,1>,<3,2>,<4,3>\}$。因此，有

$$S \circ T=\{<2,3>,<3,2>,<4,1>\}。$$

也可以直接将两个关系满足的表达式相减，得到 $S \circ T$ 的解析表示，再写出其序偶表示形式：

$$S \circ T=\{< x, z > \mid x \in X \wedge z \in Z \wedge x+z=5\}。$$

$S \circ T$ 的关系图如图 4-3 所示。

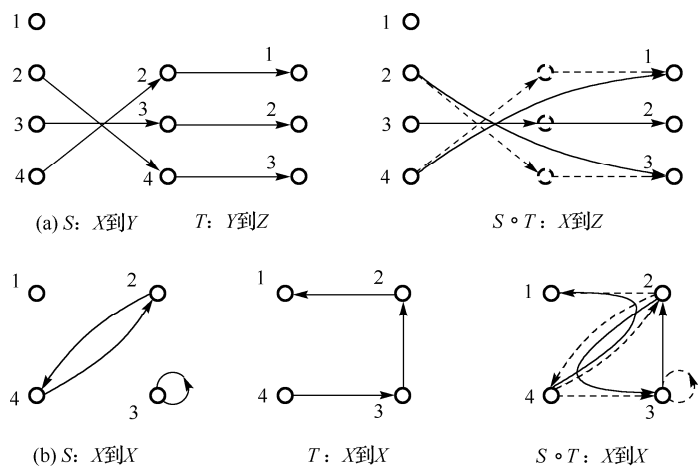


图 4-3

2．关系矩阵计算

(1) 若关系 R 的关系矩阵是 M_R，则 R^{-1} 的关系矩阵 $M_{R^{-1}}$ 是 M_R 的转置。

(2) 若关系 R、S 分别是 X 到 Y、Y 到 Z 的关系，$|X|=m$，$|Y|=n$，$|Z|=p$。记 R、S 和 $R\circ S$ 的关系矩阵分别是 $M_R=[r_{ij}]_{m\times n}$、$M_S=[s_{ij}]_{n\times p}$ 和 $M_{R\circ S}=[c_{ij}]_{m\times p}$，现在考虑元素 c_{ij} 的计算。

根据关系矩阵定义，如果 x_i 与 z_j 之间可通过某个 y_k 连接，则 c_{ij} 为 1，否则为 0。为此，需要检查每对<x_i, y_k>、<y_k, z_j>，$1\leqslant k\leqslant n$。若至少有某个 k 使 $r_{ik}=1$ 且 $s_{kj}=1$，则 c_{ij} 为 1。这可以表示为

$$c_{ij}=\sum_{k=1}^{n} r_{ik}\times s_{kj},\quad 1\leqslant i\leqslant m,\ 1\leqslant j\leqslant p。$$

由此说明，复合关系矩阵恰好是两个关系矩阵的积，即 $M_{R\circ S}=M_R\times M_S$。

直接利用算术求积和求和会导致结果可能大于 1，只要视非 0 为 1 即可。当然，也可以利用逻辑积和逻辑和计算矩阵的元素：

$$c_{ij}=\bigvee_{k=1}^{n} r_{ik}\wedge s_{kj},\quad 1\leqslant i\leqslant m,\ 1\leqslant j\leqslant p。$$

[辨析] 复合运算的实质是连接那些路长是 2 的“路”，即由两条线通过中间结点连接而成的轨迹。

例 4-8　已知集合 $A=\{1,2,3,4\}$上的关系 $R=\{<1,2>,<3,4>,<3,2>,<2,2>\}$，$S=\{<4,2>,<2,3>,<3,1>,<1,3>\}$，利用关系矩阵求 $R\circ S$。

解

$$M_R=\begin{bmatrix}0&1&0&0\\0&1&0&0\\0&1&0&1\\0&0&0&0\end{bmatrix},\quad M_S=\begin{bmatrix}0&0&1&0\\0&0&1&0\\1&0&0&0\\0&1&0&0\end{bmatrix}。$$

于是，有

$$M_{R\circ S}=\begin{bmatrix}0&0&1&0\\0&0&1&0\\0&1&1&0\\0&0&0&0\end{bmatrix}。$$

故 $R\circ S=\{<1,3>,<2,3>,<3,2>,<3,3>\}$。

[延伸] 广泛使用的关系型数据库完全以关系及其运算为理论基础，这种完善的理论基础也是关系型数据库几乎一统天下的原因。除了关系的集合运算之外，关系数据库中还定义了其他几种运算，包括选择、投影、连接和除等。例如，若 F 是一个谓词公式，R 为一个 n 元关系，则选择出满足条件 F 的行（n 元组）定义为：

$$\sigma_F(R)=\{t\mid t\in R\wedge F(t)\text{为真}\}。$$

这里的σ称为“选择运算符”，运算结果是从关系 R 中选择出满足指定条件 F 的元组，组成一个新的 n 元关系[23]。

4.2.4 多关系的复合

[定义 4-7] 设 R 是 A 上的二元关系，n 为自然数，则 R 的 n 次幂定义为：

$$\begin{cases} R^0 = I_A \\ R^{n+1} = R^n \circ R, \quad n \geqslant 0 \end{cases}。$$

由前节讨论可知，若 $<a_i, a_j> \in R^2 = R \circ R$，则 R 的关系图中存在由 a_i 到 a_j 的长度为 2 的路，自然地，若 $<a_i, a_j> \in R^{n+1} = R^n \circ R$，$n \geqslant 2$，则 R 的关系图中存在由 a_i 到 a_j 的长度为 n+1 的路。

例 4-9 若 $m \geqslant 2$，且 $<x, y> \in R^m$，则

(1) 说明由题设可推出的结论。

(2) 证明 $<y, x> \in (R^{-1})^m$。

解 (1) 因为 $R^m = R^{m-1} \circ R$，有 t_1，使

$$<x, t_1> \in R^{m-1}, \quad <t_1, y> \in R。$$

又因为 $R^{m-1} = R^{m-2} \circ R$，有 t_2，使

$$<x, t_2> \in R^{m-2}, \quad <t_2, t_1> \in R。$$

依此类推，可得到结论：存在 t_1，t_2，…，t_{m-1}，使

$$<x, t_{m-1}> \in R, <t_{m-1}, t_{m-2}> \in R, \cdots, <t_2, t_1> \in R, <t_1, y> \in R。$$

(2) 若 $<x, y> \in R^m$，由(1)的讨论可知，有

$$<y, t_1> \in R^{-1}, <t_1, t_2> \in R^{-1}, \cdots, <t_{m-2}, t_{m-1}> \in R^{-1}, <t_{m-1}, x> \in R^{-1}。$$

因此，有 $<y, x> \in (R^{-1})^m$。结论成立。

例 4-10 若 R、S 为集合 X 上的二元关系，且 $R \subseteq S$。证明：对 $m \geqslant 2$，有 $R^m \subseteq S^m$。

证明 对 $\forall <x, y> \in R^m$，有 t_1，t_2，…，$t_{m-1} \in X$，使

$$<x, t_{m-1}> \in R, <t_{m-1}, t_{m-2}> \in R, \cdots, <t_2, t_1> \in R, <t_1, y> \in R。$$

于是，有

$$<x, t_{m-1}> \in S, <t_{m-1}, t_{m-2}> \in S, \cdots, <t_2, t_1> \in S, <t_1, y> \in S。$$

因此，有 $<x, y> \in S^m$。结论成立。

[定理 4-6] 设 R 是 A 上的关系，m、n 为自然数，则

$$\begin{cases} R^m \circ R^n = R^{m+n} \\ (R^m)^n = R^{mn} \end{cases}。$$

这样的命题可以采用数学归纳法来证明。

[数学归纳法原理] 设 $p(n)$为描述自然数 n 具有某性质的谓词，$n_0 \in \mathbf{N}$ 为一个起始值。若

(1) $p(n_0)$为真；

(2) 对 $\forall n \in \mathbf{N}$ 且 $n \geqslant n_0$，若 $p(n)$为真，则可证明 $p(n+1)$为真。

那么，必有对 $\forall n \in \mathbf{N}$ 且 $n \geqslant n_0$，$p(n)$为真。

证明　对于定理中的命题 $R^m \circ R^n = R^{m+n}$，假定 m 已给定，对 n 进行归纳。

若 n=0，$R^m \circ R^0 = R^m \circ I_A = R^m = R^{m+0}$。

假定 $R^m \circ R^n = R^{m+n}$，$R^m \circ R^{n+1} = R^m \circ R^n \circ R^1 = R^{m+n} \circ R = R^{m+n+1}$。故结论成立。

另一个命题的证明类似。

[定理 4-7] 设 $|A|=n$，R 是 A 上的二元关系，则存在自然数 s 和 t，$s<t$，使得 $R^s = R^t$。

证明　因 R 是 A 上的关系，对任意的自然数 n，R^n 都是 $A \times A$ 的子集。因为 $|A \times A| = n^2$，$|\mathscr{P}(A \times A)| = 2^{n^2}$，即 $A \times A$ 仅有 2^{n^2} 个不同子集。因此，只要记 $t = 2^{n^2}+1$，则 R^t 必然与 $R \sim R^{t-1}$ 中的某个关系重复，即有 $1 \leqslant s \leqslant 2^{n^2} < t$，使得 $R^s = R^t$。

[定理 4-8] *设 R 是 A 上的二元关系，若存在自然数 s 和 t，$s<t$，使得 $R^s = R^t$，则

(1) 对任意自然数 k，有 $R^{s+k} = R^{t+k}$。

(2) 对任意自然数 k 和 i，有 $R^{s+kp+i} = R^{s+i}$，其中 $p = t - s$。

(3) 记 $S = \{R^0, R^1, \cdots, R^{t-1}\}$，则对任意自然数 m，有 $R^m \in S$。

证明　定理中的(1)是显然的，(2)可用归纳法证明。这里仅证明(3)。

对于任意的自然数 m，若 $m < t$，结论自然成立。否则，有 $m \geqslant t$，即 $m - s \geqslant p$。于是，存在正整数 k 和 $0 \leqslant r < p$，使 $m - s = kp + r$，即 $m = s + kp + r$。由(2)，有

$$R^m = R^{s+r}。$$

因为 $s + p = t$，而 $s + r < s + p \leqslant t - 1$，故 $R^{s+r} \in S$，即 $R^m \in S$。结论成立。

上述定理说明 R 的幂呈周期性变化。如果 s 和 t 是满足 $R^s = R^t$ 的一对最小自然数，则 R 的幂最多有 t 个不同值，以后的值将按 $t - s$ 为周期重复。因此，可以将高次幂化简为低次幂。

例 4-11　设 R 的关系矩阵为：

$$M_R = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}。$$

求 R^m 的重复周期，并计算 R^{35}。

解　由 M_R，有

$$M_R^2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}，M_R^3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}，M_R^4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}。$$

由于 $R^2 = R^4$，这说明 R 至多有 4 个不同的幂次 $R^0 \sim R^3$，重复周期为 $4-2=2$。

又因为 $35 = 2+16\times 2+1$，可见 $R^{35} = R^{2+1} = R^3$。

思考与练习 4.2

4-7 若 X、Y、Z 为集合，R 和 S 分别是 X 到 Y、Y 到 Z 的关系，且 $<a,b>\in R$，$<b,c>\in S$，能得到什么结论？若还有 $<b,b>\in S$，又能得到什么结论？

4-8 若 $R = \{<1, 2>, <2, 1>\}$，$S=\{<1, 1>, <2, 2>, <2, 3>\}$，求 $R\circ S$。

4-9 设 $R = \{<x, y>| x, y\in \mathbf{N}$ 且 $x+3y = 12\}$，求 R^2。

4-10 有 $X = \{0,1,2,3\}$上的关系 $f = \{<i, j>|j = i+1$或$j = i/2\}$，$g = \{<i, j>|i = j+2\}$，求 $f\circ g$、$g\circ f$、f^2、g^2、$f\circ g\circ f$ 和 $g\circ f\circ g$。

4-11 设 R、S 是集合 A 到 B 的关系，证明：

(a) $(R\bigcup S)^{-1} = R^{-1}\bigcup S^{-1}$。 (b) $(R\bigcap S)^{-1} = R^{-1}\bigcap S^{-1}$。

(c) $(A\times B)^{-1} = B\times A$。 (d) $(\sim R)^{-1} = \sim (R^{-1})$。

4-12 设 R、S 是 X 上的关系，证明：$R^m \subseteq (R\bigcup S)^m$，$m$ 为任意正整数。

4-13 设 $R\subseteq A\times A$ 且 $<a,b>\in R\circ I_A$，证明 $<a,b>\in R$。

4-14 设 R 是集合 A 到 B 的关系，证明 $I_A\circ R = R\circ I_B = R$。

4-15 设 R、S、T 是任意关系，证明：

(a) $(R\circ S)\circ T = R\circ (S\circ T)$。 (b) $(R\circ S)^{-1} = S^{-1}\circ R^{-1}$。

4-16 利用关系矩阵计算习题 4-10 中的 f^2，并求出 f^m 的重复周期。

4-17 有 $A = \{a,b,c,d\}$上的关系 $R = \{<b,b>,<b,c>,<c,a>\}$，计算 $\bigcup_{i=1}^{+\infty} R^i$。

4.3 关系的性质

很多关系具有一定的特殊性，这使其表现为某种特殊的关系。在一些应用中，常常希望关系具有这些性质，也需要正确判定一个关系是否具有这些性质。

4.3.1 自反与反自反关系

[定义 4-8] 设 R 是 X 上的二元关系。若对所有的 $x\in X$，有 $<x,x>\in R$，则称 R 是 X 上的**自反关系**（reflexive relation）。符号描述为：

$$R \text{ 是 } X \text{ 上的自反关系} \Leftrightarrow \forall x(x\in X \rightarrow <x,x>\in R)。$$

[辨析] 定义要求对所有的 $x\in X$，都有 $<x,x>\in R$，或者说只要 $x\in X$，就有 $<x,x>\in R$。其他性质也都类似。

[定义 4-9] 设 R 是 X 上的二元关系。若对所有的 $x\in X$，有 $<x,x>\notin R$，则称 R 是 X 上的**反**

自反关系（irreflexive relation）。符号描述为：

$$R \text{ 是 } X \text{ 上的反自反关系} \Leftrightarrow \forall x(x \in X \rightarrow < x, x > \notin R)。$$

例如，实数集上的≥、≤、=关系，集合上的=、$\subseteq$关系，以及任何集合 X 上的恒等关系 I_X 都是自反关系，整数集上的>、≠关系和集合上的$\subset$关系都是反自反关系。

定义中的“任意性”要求非常关键。例如，$A=\{a, b, c\}$，$R=\{<a, a>, <b, b>\}$不是自反的，因为缺少序偶$<c, c>$，$S=\{<a, a>, <b, b>, <c, c>, <a, c>\}$才是自反的。

[理解] 如何判定一个关系具有某种性质？其实，每个性质的定义都由一个条件句命题来描述，只要证明此命题为真。而如果条件句的前件为 0，则命题必为 1，故定义满足。

例 4-12　找出一个关系，既不是自反的，也不是反自反的。能再找出一个关系，既是自反的，也是反自反的吗？

解　若 $A=\{1,2,3\}$，则 $R=\{<1,1>,<2,2>\}$既不是自反的，也不是反自反的。

比较自反性和反自反性定义的两个条件句：

$$x \in X \rightarrow < x, x > \in R,$$
$$x \in X \rightarrow < x, x > \notin R。$$

显然，两个条件句的后件是矛盾的。因此，要使它们同时为真，只有使前件 $x \in X$ 为假，唯一的选择是 $X=\varnothing$。此时，关系 R 也必然是空集。可见，只有定义在空集合 Ø 上的空关系 Ø 才既是自反，也是反自反的。

[辨析] 使一个定义中条件句的前件为假，从而使定义得到满足是一个常见且十分重要的问题，也是能够正确判定一个性质是否被满足的基本保证。

[辨析] “反自反”不等于“不自反”。满足自反性要求关系包含所有形如$<x, x>$的序偶，满足反自反性要求关系不能包含任何一个形如$<x, x>$的序偶。仅包含部分$<x, x>$而不是全部就什么都不是。

4.3.2　对称与反对称关系

[定义 4-10] 设 R 是 X 上的二元关系。对任意的 $x,y \in X$，若 $< x, y > \in R$，就有 $< y, x > \in R$，则称 R 是 X 上的**对称关系**（symmetric relation）。符号表示为：

$$R \text{ 是 } X \text{ 上的对称关系} \Leftrightarrow \forall x \forall y((x \in X \wedge y \in X \wedge < x, y > \in R) \rightarrow < y, x > \in R)。$$

例如，任何集合上的空关系是对称关系，而定义在集合 $A=\{1,2,3\}$上的关系 $R=\{<1, 1>, <1, 2>, <2, 1>\}$是对称关系，但 $S=\{<1, 2>, <2, 1>, <1, 3>\}$不是对称关系，因为$<3,1> \notin S$。

例 4-13　设 $A=\{2,3,5,7\}$，A 上的关系 $R=\{< x, y > | (x-y)/2 \text{是偶数}\}$，证明 R 是 A 上的自反和对称关系。

证明　对 $\forall x \in A$，有 $(x-x)/2=0$，即 $< x, x > \in R$，故 R 是自反的。

对 $\forall x, y \in A$，若 $< x, y > \in R$，则有偶数 k，使 $(x-y)/2=k$。因为 $-k$ 也是偶数，且有

$$(y-x)/2=-k\ 。$$

知$<y,x>\in R$。故 R 是对称的。

[定义 4-11] 设R是X上的二元关系。对任意的$x,y\in X$,若$<x,y>\in R$且$x\neq y$,就有$<y,x>\notin R$,则称 R 是 X 上的**反对称关系**（antisymmetric relation）。符号表示为：

R 是 X 上的反对称关系 $\Leftrightarrow \forall x\forall y((x\in X\wedge y\in X\wedge <x,y>\in R\wedge x\neq y)\rightarrow <y,x>\notin R)$。

日常使用的大量关系都是反对称关系，如≤、≥和⊆等。例如，对于≤，满足

只要 $a\leqslant b$，且 $a\neq b$，必有 $b\not\leqslant a$。

不过，对这种性质更一般的描述为

只要 $a\leqslant b$ 且 $b\leqslant a$，则 $a=b$。

这是因为

$$\begin{aligned}&(<x,y>\in R\wedge x\neq y)\rightarrow <y,x>\notin R\\ &\Leftrightarrow \neg(<x,y>\in R\wedge x\neq y)\vee <y,x>\notin R\\ &\Leftrightarrow \neg(<x,y>\in R\wedge <y,x>\in R)\vee x=y\\ &\Leftrightarrow (<x,y>\in R\wedge <y,x>\in R)\rightarrow x=y\ 。\end{aligned}$$

由此，可以将原定义转换成另一种等价的描述方式：

R 是 X 上的反对称关系 $\Leftrightarrow \forall x\forall y((x\in X\wedge y\in X\wedge <x,y>\in R\wedge <y,x>\in R)\rightarrow x=y)$。

[辨析] 在实际证明时，后一种定义描述形式常常更容易叙述。

例 4-14 正整数集 $\mathbf{Z}^+$上的整除关系$|=\{<x,y>|x,y\in\mathbf{Z}^+$且 y 能被 x 整除$\}$是反对称关系。

证明 若$a|b$且$b|a$，则有

$$a\leqslant b，且\ b\leqslant a。$$

于是，有 $a=b$。所以，$|$是反对称关系。

此外，整除关系|也是自反的，因为任何整数都能整除自己。

例 4-15 找出一个关系，既不是对称的，也不是反对称的；再找出一个关系，既是对称的，又是反对称的。

解 $A=\{a,b,c\}$，$R=\{<a,b>,<b,a>,<a,c>\}$既不是对称的，也不是反对称的。因为缺少$<c,a>$，破坏了对称性，而包含成对序偶$<a,b>$和$<b,a>$破坏了反对称性。

任意一个集合上的空关系既是对称的，也是反对称的。这是因为定义中的$<x,y>\in R$为假，条件句$<x,y>\in R\rightarrow <y,x>\in R$和$(<x,y>\in R\wedge x\neq y)\rightarrow <y,x>\notin R$都为真。

集合 $A=\{1,2\}$上的 $R=\{<1,1>\}$和任意集合 A 上的关系 I_A 是对称的，也是反对称的。这是因为 R 和 I_A 仅含有$<x,x>$形式的序偶，条件句$<x,y>\in R\rightarrow <y,x>\in R$为真，而反对称定义中的条件句前件$<x,y>\in R\wedge x\neq y$为假，故条件句$(<x,y>\in R\wedge x\neq y)\rightarrow <y,x>\notin R$为真。

[辨析] “反对称”不等于“不对称”。一个关系 R 中形如$<x,x>$的序偶与对称性和非对称性都无关联。

4.3.3　传递关系

[定义 4-12]　设 R 是 X 上的二元关系。对任意的 $x,y,z\in X$，若 $<x,y>\in R$ 且 $<y,z>\in R$，就有 $<x,z>\in R$，则称 R 是 X 上的（可）**传递关系**（transitive relation）。符号表示为：

$$R \text{ 是 } X \text{ 上的传递关系} \Leftrightarrow \forall x\forall y\forall z((x\in X\wedge y\in X\wedge z\in X\wedge xRy\wedge yRz)\rightarrow xRz)。$$

实数集 **R** 上的≤、<、≥、>、=和集合的包含关系 $\subseteq$ 都是传递关系，通常的描述是

若 $a\leqslant b$ 且 $b\leqslant c$，则 $a\leqslant c$。

若 $A\subseteq B$ 且 $B\subseteq C$，则 $A\subseteq C$。

例 4-16　若 $A=\{a,b,c\}$，问 $r_1=\varnothing$，$r_2=\{<a,a>\}$，$r_3=\{<a,b>,<a,c>\}$，$r_4=\{<a,a>,<a,b>,<b,a>\}$，$r_5=\{<a,a>,<a,b>,<a,c>,<b,c>\}$是传递关系吗？

解　r_1 和 r_3 是传递关系，因为不存在具有相同 y 的一对序偶，定义中条件句的前件 $xRy\wedge yRz$ 为假，故 $xRy\wedge yRz\rightarrow xRz$ 为真。r_2 是传递关系，相当于定义中 $x=y=z=a$。r_4 不是传递关系，因为存在<b,a>和<a,b>，但不存在<b,b>。r_5 是传递关系，相当于定义中 $x=y=a$，$z=b$ 或 c。

[理解] 对传递关系的通俗解释是，所有可连接的序偶其连接后的结果都属于此关系。

4.3.4　特殊关系的判定

1．充分必要条件

在理论上容易总结出几种关系性质应满足的条件，依据这些条件可以对关系是否具有某种性质进行判定。

[定理 4-9] 设 R 是 A 上的二元关系，则

(1) R 是自反关系当且仅当 $I_A\subseteq R$。

(2) R 是反自反关系当且仅当 $R\bigcap I_A=\varnothing$。

(3) R 是对称关系当且仅当 $R=R^{-1}$。

(4) R 是反对称关系当且仅当 $R\bigcap R^{-1}\subseteq I_A$。

(5) R 是传递关系当且仅当 $R\circ R\subseteq R$，即 $R^2\subseteq R$。

证明　(1) ① R 是自反关系$\vdash I_A\subseteq R$，即推证集合包含。

对 $\forall <x,y>$，有

$$<x,y>\in I_A\Rightarrow x=y\Rightarrow_{(R\text{的自反性})}<x,y>\in R。$$

② $I_A\subseteq R\vdash R$ 是自反关系，即验证自反性。

对 $\forall x$，有

$$x\in A\Rightarrow <x,x>\in I_A\Rightarrow_{(I_A\subseteq R)}<x,x>\in R。$$

(2) ① R 是反自反关系$\vdash R\bigcap I_A=\varnothing$，即推证集合相等（互相包含）。

若有 $<x,y>\in R\bigcap I_A$，则 $<x,y>\in R$ 且 $<x,y>\in I_A$（即 x=y）。故 $<x,x>\in R$，与反自反性矛盾，故 $R\bigcap I_A=\varnothing$。

② $R \cap I_A = \varnothing \vdash R$ 是反自反关系，即验证反自反性。

对 $\forall x$，有

$$x \in A \Rightarrow_{(I_A\text{定义})} < x,x > \in I_A \Rightarrow_{(R \cap I_A = \varnothing)} < x,x > \notin R \text{。}$$

(3) ① R 是对称关系 $\vdash R = R^{-1}$，即推证集合互相包含。

对 $\forall < x,y >$，有

$$< x,y > \in R \Leftrightarrow_{(R\text{的对称性})} < y,x > \in R \Leftrightarrow_{(R^{-1}\text{的定义})} < x,y > \in R^{-1} \text{。}$$

② $R = R^{-1} \vdash R$ 是对称关系，即验证对称性。

对 $\forall < x,y >$，有

$$< x,y > \in R \Rightarrow_{(R=R^{-1})} < x,y > \in R^{-1} \Leftrightarrow_{(R^{-1}\text{的定义})} < y,x > \in R \text{。}$$

(4) ① R 是反对称关系 $\vdash R \cap R^{-1} \subseteq I_A$，即推证集合包含。

对 $\forall < x,y >$，有

$$\begin{aligned} < x,y > \in R \cap R^{-1} &\Rightarrow_{(\text{集合交定义})} < x,y > \in R \wedge < x,y > \in R^{-1} \\ &\Rightarrow_{(R^{-1}\text{的定义})} < x,y > \in R \wedge < y,x > \in R \\ &\Rightarrow_{(R\text{的反对称性})} x = y \\ &\Rightarrow < x,y > \in I_A \text{。} \end{aligned}$$

② $R \circ R^{-1} \subseteq I_A \vdash R$ 是反对称关系，即验证反对称性。

对 $\forall < x,y >$，有

$$\begin{aligned} < x,y > \in R \wedge < y,x > \in R &\Rightarrow_{(R^{-1}\text{的定义})} < x,y > \in R \wedge < x,y > \in R^{-1} \\ &\Rightarrow_{(\text{集合交定义})} < x,y > \in R \cap R^{-1} \\ &\Rightarrow_{(R \cap R^{-1} \subseteq I_A)} < x,y > \in I_A \\ &\Rightarrow x = y \text{。} \end{aligned}$$

(5) ① R 是传递关系 $\vdash R \circ R \subseteq R$，即推证集合包含。

对 $\forall < x,y >$，有

$$< x,y > \in R \circ R \Rightarrow_{(\text{复合关系定义})} \exists t(< x,t > \in R \wedge < t,y > \in R) \Rightarrow_{(R\text{的传递性})} < x,y > \in R \text{。}$$

② $R \circ R \subseteq R \vdash R$ 是传递关系，即验证传递性。

对 $\forall < x,y >$ 和 $< y,z >$，有

$$< x,y > \in R \wedge < y,z > \in R \Rightarrow_{(\text{复合关系定义})} < x,z > \in R \circ R \Rightarrow_{(R \circ R \subseteq R)} < x,z > \in R \text{。}$$

例 4-17 若有整数 $m \geqslant 2$ 和二元关系 R，使得

$$< x,t_{m-1} > \in R, < t_{m-1},t_{m-2} > \in R, \cdots, < t_2,t_1 > \in R, < t_1,y > \in R \text{。}$$

可以得到什么结论？若 R 是传递关系，又可得到什么结论？

解 对于一般的关系 R，逐次利用关系复合运算，可推出结论 $< x,y > \in R^m$。

若 R 具有传递性时，可推出结论 $< x,y > \in R$。

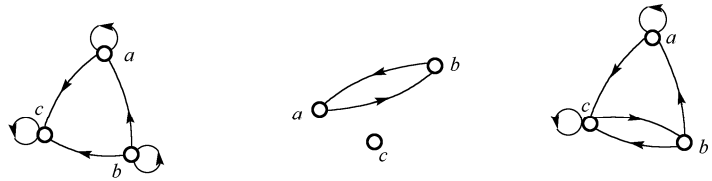
事实上，若 R 是传递关系，$R^m \subseteq R$ 对所有整数 $m \geqslant 1$ 成立。这说明一个传递关系自身的复合不可能产生新的序偶。

2．利用关系图的性质判别

(1) 自反关系的每个元素都有自环，反自反关系的每个元素都没有自环。仅有部分而非全部自环时既不是自反关系也不是反自反关系。

(2) 对称关系的连线都是成对的，反对称关系的连线都是不成对的。同时包含成对和不成对连线的关系既不是对称关系，也不是反对称关系；没有不相同元素之间连线时既是对称关系，也是反对称关系。

(3) 传递关系表现为，对任何两个元素 x 和 y，如果可以通过一条“路”从 x 到达 y，则直接有 x 与 y 的连线。图 4-4 显示了几种关系的关系图示例，$A = \{a, b, c\}$。



(a) 自反，反对称，传递　　(b) 反自反，对称　　(c) 不满足任何性质

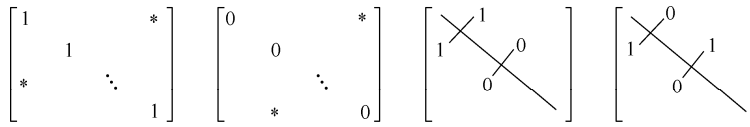
图 4-4

3．利用关系矩阵的性质判别

(1) 自反关系的关系矩阵的主对角线都是 1，反自反关系矩阵主对角线都是 0。主对角线元素同时存在 1 和 0 时既不是自反关系也不是反自反关系。

(2) 对称关系的关系矩阵为对称矩阵，反对称关系的关系矩阵则关于主对角线严格不对称。主对角线元素与对称性和反对称性无关，因为它是“轴”。

图 4-5 说明了几种关系的关系矩阵特点。



(a) 自反　　(b) 反自反　　(c) 对称　　(d) 反对称

图 4-5

思考与练习 4.3

4-18　分别用自然语言和符号描述关系的自反性、反自反性、对称性、反对称性和传递性。

4-19　设有集合 $A = \{1,2,3\}$ 上定义的如下关系，它们是自反、反自反、对称、反对称和传递的吗？

(a) $R=\{<1,1>\}$。 (b) $S=\{<1,2>,<2,1>\}$。

(c) $T=\{<1,2>, <3,2>, <3,3>\}$。

4-20 举出一个关系示例，使其分别满足：

(a) 既不是自反的，也不是反自反的。 (b) 既是自反的，也是反自反的。

(c) 既不是对称的，也不是反对称的。 (d) 既是对称的，也是反对称的。

4-21 设 $A=\{a, b, c\}$，给出 A 上的一个二元关系 R，使其不满足自反、反自反、对称、反对称和传递性中的任何一种性质。

4-22 若 α 和 β 是集合 X 上的关系，证明或否定：当 α 和 β 分别具有自反、反自反、对称、反对称和传递性时，$\alpha\cap\beta$ 和 $\alpha\cup\beta$ 也分别具有相同的性质。

4-23 若 α 和 β 是集合 X 上的关系，证明或否定：当 α 和 β 分别具有自反、反自反、对称和传递性时，$\alpha\circ\beta$ 也分别具有相同的性质。

4-24 若 R 是 X 上的自反二元关系，且对任意的 x，y，$z\in X$，若 xRy 且 yRz，则 zRx。证明 R 是对称和传递的。

4-25 若 $R\subseteq A\times A$，证明或否定：若 R 分别是自反、反自反、对称、反对称或传递关系，则 R^{-1} 也分别具有相同的性质。

4-26 若 R 是可传递的二元关系，证明或否定：

(a) $R\cap R^{-1}$ 是可传递的。 (b) $R\cup R^{-1}$ 是可传递的。

(c) $R-R^{-1}$ 是可传递的。 (d) $R^{-1}-R$ 是可传递的。

4-27 若 R 是 A 上的反对称关系，$|A|=n$，在 $R\cap R^{-1}$ 的关系矩阵中可能有多少个非零值？

4-28 n 个元素的集合 A 上存在多少个不同的自反关系？

4-29 设 R 是 A 上的关系，若 R 是自反的和传递的，则 $R^2=R$。其逆命题也成立吗？

4.4 关系的闭包

关系的自反性、对称性和传递性是实际应用中经常需要的性质。当一个关系不满足这些性质时，一定是因为缺少某些序偶所致。因此，需要在关系中适当增加序偶，以使其具有相应的性质。很明显，对于任意集合 X，全关系 $X\times X$ 显然是自反、对称和传递的，我们当然不希望将 X 上的关系 R 都扩充成全关系。因此，这种扩充应恰好使关系 R 具有所需要的性质为止。

4.4.1 闭包的概念

通常，对关系 R 扩充后得到的新关系 S 应恰好具有想要的性质，这被称为 S 对该性质封闭，且 S 显然包含了 R。因此，称 S 是 R 的**闭包**（closure）。

[定义 4-13] 设 R 是 X 上的二元关系，如果有一个关系 S 满足：

(a) S 是自反（对称、传递）的；

(b) $R\subseteq S$；

(c) 对于 X 上的所有自反（对称、传递）关系 T，若 $R\subseteq T$，就有 $S\subseteq T$，则称 S 是 R 的**自反**

闭包（**r**eflexive closure）（对称闭包（**s**ymmetric closure）、传递闭包（**t**ransitive closure）），记作 $r(R)$（$s(R)$、$t(R)$）。

[辨析] 定义中的(c)也称为“最小性”，它说明闭包是使 R 刚好被扩充到具有所需某种性质为止。

[理解] 通俗地讲，R 的自反（对称、传递）闭包是指具有自反性（对称性、传递性）且包含 R 的“最小”关系。这里的小于是以集合包含来衡量的，即 R 小于等于 S 是指 $R \subseteq S$。

例如，$X=\{1,2,3\}$，$R=\{<1,1>,<2,2>,<1,3>\}$不具有自反性。$S=\{<1,1>,<2,2>,<3,3>,<1,3>\}$是 R 的自反闭包，但 $T=\{<1,1>,<2,2>,<3,3>,<1,3>,<3,1>\}$不是 R 的自反闭包，因为它虽然满足(a)、(b)规则，但不是最小关系，即不满足规则(c)。

[定理 4-10] 若 R 是 X 上的二元关系，则

(1) R 是自反的，当且仅当 $r(R)=R$。

(2) R 是对称的，当且仅当 $s(R)=R$。

(3) R 是传递的，当且仅当 $t(R)=R$。

这说明当 R 具有自反性（对称性、传递性）时，本身就是自己的自反（对称、传递）闭包，因为它自己是满足定义 4-13(a)、(b)规则的“最小”关系。

4.4.2　闭包计算

[定理 4-11] 设 R 是 X 上的二元关系，则

(1) $r(R)=R\cup I_X$。

(2) $s(R)=R\cup R^{-1}$。

(3) $t(R)=\bigcup_{k=1}^{+\infty}R^k=R\cup R^2\cup R^3\cup\cdots$，$\bigcup_{k=1}^{+\infty}R^k$ 也记为 R^+。

闭包的证明就是逐条验证定义中的 3 条规则，但一般(b)是显然的，仅需要验证(a)与(c)。

证明　(1)记 $S=R\cup I_X$。

(a) 对 $\forall x\in X$，因 $<x,x>\in I_X$，有 $<x,x>\in S$，故 S 是自反的。

(c) 对 X 上的自反关系 T，若 $R\subseteq T$，推证 $S\subseteq T$。

对 $\forall <x,y>\in S$，有

$$<x,y>\in R\vee <x,y>\in I_X。$$

若前者为真，因 $R\subseteq T$，有 $<x,y>\in T$。若后者为真，有 $x=y$。因 T 是自反关系，有 $<x,y>\in T$。总之，$S\subseteq T$。

(2) 记 $S=R\cup R^{-1}$。

(a) 对 $\forall <x,y>$，有

$$<x,y>\in S\Rightarrow <x,y>\in R\vee <x,y>\in R^{-1}$$

$$\Rightarrow <y,x>\in R^{-1}\vee <y,x>\in R\Rightarrow <y,x>\in S。$$

故 S 是对称的。

(c) 对 X 上的对称关系 T，若 $R\subseteq T$，推证 $S\subseteq T$。

对 $\forall < x,y > \in S$，有

$$< x,y > \in R \vee < x,y > \in R^{-1}。$$

若前者为真，因 $R \subseteq T$，有 $< x,y > \in T$。若后者为真，有 $< y,x > \in R$。因 $R \subseteq T$，有 $< y,x > \in T$。又因 T 是对称关系，有 $< x,y > \in T$。总之，$S \subseteq T$。

(3) 记 $S = R \cup R^2 \cup R^3 \cup \cdots$。

(a) 对 $\forall < x,y > \in S, < y,z > \in S$，有正整数 m 和 n，使

$$< x,y > \in R^m，< y,z > \in R^n。$$

于是，有 $< x,z > \in R^m \circ R^n = R^{m+n}$，即 $< x,z > \in S$，故 S 是传递的。

(c) 对 X 上的传递关系 T，若 $R \subseteq T$，推证 $S \subseteq T$。

对 $\forall < x,y > \in S$，有正整数 m，使 $< x,y > \in R^m$。因此，有 t_1，t_2，…，t_{m-1}，使

$$< x,t_1 > \in R, < t_1,t_2 > \in R, \cdots, < t_{m-2},t_{m-1} > \in R, < t_{m-1},y > \in R。$$

因 $R \subseteq T$，有

$$< x,t_1 > \in T, < t_1,t_2 > \in T, \cdots, < t_{m-2},t_{m-1} > \in T, < t_{m-1},y > \in T。$$

因 T 是传递的，有 $< x,y > \in T$。故 $S \subseteq T$。

事实上，由于有限集上的关系 R 的幂存在周期性，式(3)不必计算到无穷。

[定理 4-12] 若 $|X| = n$，R 是 X 上的二元关系，则存在一个正整数 $m \leqslant n$，使得

$$t(R) = \bigcup_{k=1}^{m} R^k = R \cup R^2 \cup R^3 \cup \cdots \cup R^m。$$

证明 因为 $\bigcup_{k=1}^{m} R^k \subseteq R^+$，故只需要证明 $R^+ \subseteq \bigcup_{k=1}^{m} R^k$。

若 $< x,y > \in R^+$，必有 p 使得 $< x,y > \in R^p$。因 R 幂次的周期性，满足上述关系的 p 可以很多，但若记最小的 p 为 m，则必有 $m \leqslant n$。

否则，若 $m > n$。记 $t_0 = x$，$t_m = y$，则存在 t_1，t_2，…，t_{m-1}，使

$$t_0 R t_1，\ t_1 R t_2, \cdots，\ t_{m-2} R t_{m-1}，\ t_{m-1} R t_m。$$

因为上述序列中共 $m+1$（$m+1 > n$）个元素，但 X 只有 n 个元素，故必存在 $0 \leqslant a < b \leqslant m$，使得 $t_a = t_b$，原序偶序列为：

$$t_0 R t_1，\ t_1 R t_2, \cdots，\ t_{a-1} R t_a, \underbrace{t_a R t_{a+1}, \cdots，\ t_{b-1} R t_b}_{\text{因}t_a = t_b\text{而多余的序偶}}，\ t_b R t_{b+1}, \cdots，\ t_{m-1} R t_m。$$

在序列中除去<t_a,t_{a+1}>至<t_{b-1},t_b>之间的序偶再重新连接，仍有 $< x,y > \in R^{m-(b-a)}$，这与 m 最小的假设矛盾。结论成立。

[辨析] 此定理说明，若 $|X| = n$，传递闭包至多需要计算到 R^n 即可。因此，定理可写成 $t(R) = \bigcup_{k=1}^{n} R^k$。

[延伸] 在一个图中，如果从元素 x 可途径若干条连线连接到元素 y，称 x 到 y 是可达的。因

此，传递闭包的实质是确定任意两点间是否可达，故其关系矩阵也称为“可达矩阵”。在一个大型网络中，主机等设备代表着元素，而他们之间的有线和无线网络构成了连线，进而形成了关系图。可达矩阵在衡量该图的网络状态及在主机之间是否可通信过程中起着重要作用[2]。

本质上，定理中的传递闭包计算就是将能够可达的两个元素之间直接用连线相连，这种过程要循环测试，直到不再有新连线加入为止，时间消耗非常大，但利用 Warshall 算法可以有效降低求和的复杂性，提高效率，参见图 4-6。

```
T=MR;                          /*T 为传递闭包的关系矩阵，n 为集合元素个数 */
for(k=1; k≤n; k=k+1)
    for(i=1; i≤n; i=i+1)
        for(j=1; j≤n; j=j+1)
            if(T[i][k] == 1 && T[k][j] == 1)
                T[i][j] = 1;
```

图 4-6

用 I_R 表示单位矩阵，M_R^{T} 为 M_R 的转置，根据定理，在利用关系矩阵计算闭包时，有

$$M_{r(R)} = M_R + I_R ,$$

$$M_{s(R)} = M_R + M_R^{\mathrm{T}} ,$$

$$M_{t(R)} = \sum_{k=1}^{n} M_R^k 。$$

这里的矩阵加法和乘法都是逻辑运算。

从关系图上看，自反闭包是为每个结点添上自环，对称闭包为每条线段加上箭头相反的连线，传递闭包将所有可达的结点对之间用连线直接相连。

例 4-18　若 $A=\{a,b,c\}$，A 上的关系 $R=\{<a,b>,<b,c>,<c,a>\}$，求 $r(R)$、$s(R)$和 $t(R)$。

解　$r(R)=R\cup I_A=\{<a,a>,<b,b>,<c,c>,<a,b>,<b,c>,<c,a>\}$。

$s(R)=R\cup R^{-1}=\{<a,b>,<b,c>,<c,a>,<b,a>,<c,b>,<a,c>\}$。

因为

$$M_R=\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix},\quad M_{R^2}=\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix},\quad M_{R^3}=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix},\quad M_{R^4}=M_R 。$$

得 $M_{t(R)}=\sum_{k=1}^{3}M_{R^k}=\begin{bmatrix}1&1&1\\1&1&1\\1&1&1\end{bmatrix}$，即 $t(R)=A\times A$。

例 4-19　设 R 是集合 X 上的二元关系，则

(1) $rs(R)=sr(R)$。　　(2) $rt(R)=tr(R)$。

(3) $st(R)\subseteq ts(R)$。

证明 题目仍是证明集合包含。

(1) 可直接采用集合算律证明。

$$rs(R)=s(R)\cup I_X=R\cup R^{-1}\cup I_X=(R\cup I_X)\cup(R^{-1}\cup I_X)=r(R)\cup r(R)^{-1}=sr(R)。$$

(2) 推证 $rt(R)\subseteq tr(R)$。

对 $\forall <x,y>$，若 $<x,y>\in rt(R)$，因 $rt(R)=t(R)\cup I_X$，有

$$<x,y>\in t(R)\text{或}<x,y>\in I_X。$$

若前者为真，有 m 使 $<x,y>\in R^m$。因 $R\subseteq R\cup I_X$，有

$$<x,y>\in (R\cup I_X)^m。$$

知 $<x,y>\in tr(R)$。

若后者为真，有 $<x,y>\in R\cup I_X$，知 $<x,y>\in tr(R)$。

类似地，可证明 $tr(R)\subseteq rt(R)$。结论成立。

(3) 对 $\forall <x,y>\in st(R)=t(R)\cup t(R)^{-1}$，有

$$<x,y>\in t(R)\text{ 或 }<x,y>\in t(R)^{-1}。$$

若前者为真，有 m 使 $<x,y>\in R^m$。因 $R\subseteq R\cup R^{-1}$，有

$$<x,y>\in (R\cup R^{-1})^m。$$

知 $<x,y>\in ts(R)$。

若后者为真，有 $<y,x>\in t(R)$。因此，有 n 使 $<y,x>\in R^n$。于是，有

$$<x,y>\in (R^{-1})^n。$$

因 $R^{-1}\subseteq R\cup R^{-1}$，有

$$<x,y>\in (R\cup R^{-1})^n。$$

知 $<x,y>\in ts(R)$。故 $st(R)\subseteq ts(R)$ 成立。

思考与练习 4.4

4-30 设集合 $A=\{a,b,c,d\}$ 上的关系 $R=\{<a,b>,<b,a>,<b,c>,<c,d>\}$，利用关系图和关系矩阵求出 R 的自反闭包、对称闭包和传递闭包。

4-31 设有集合 $A=\{a,b,c,d\}$ 上的关系 $R=\{<a,b>,<b,c>,<c,a>,<c,d>\}$，求 $rt(R)$。

4-32 对于整数集 $\mathbf{Z}$ 上的关系 $R=\{<x,y>\mid x,y\in\mathbf{Z}\text{且}y=x+1\}$，说明 R 的传递闭包 $t(R)$是小于关系“<”。

4-33 设 α 和 β 是集合 X 上的关系且 $\alpha\subseteq\beta$，证明：

(a) $r(\alpha)\subseteq r(\beta)$。 (b) $s(\alpha)\subseteq s(\beta)$。

(c) $t(\alpha) \subseteq t(\beta)$。

4-34　设 α 和 β 是集合 X 上的关系，证明：

(a) $r(\alpha \cup \beta) = r(\alpha) \cup r(\beta)$。　　(b) $s(\alpha \cup \beta) = s(\alpha) \cup s(\beta)$。

(c) $t(\alpha) \cup t(\beta) \subseteq t(\alpha \cup \beta)$。

并举例说明 $t(\alpha \cup \beta) \neq t(\alpha) \cup t(\beta)$。

4-35　设 $R \subseteq A \times A$，证明：

(a) 若 R 是自反的，则 $s(R)$和 $t(R)$是自反的。

(b) 若 R 是对称的，则 $r(R)$和 $t(R)$是对称的。

(c) 若 R 是传递的，则 $r(R)$是传递的，但 $s(R)$不一定是传递的。

4-36　设 $R \subseteq A \times A$，证明：

(a) 若 R 是反自反的，则 $s(R)$是反自反的，但 $t(R)$不一定是反自反的。

(b) 若 R 是反对称的，则 $r(R)$是反对称的，但 $t(R)$不一定是反对称的。

4-37　举例说明 $st(R) \neq ts(R)$。

4.5　相容关系与等价关系

4.5.1　集合的覆盖与划分

对于一个大的数据集，经常需要根据一定的性质将其划分为不同的部分，进而分别研究元素之间的关系。

[定义 4-14]　若 A 为非空集合，$S = \{S_1, S_2, \cdots, S_m\}$，满足：

(a) $S_i \subseteq A$，$1 \leqslant i \leqslant m$，

(b) $S_i \neq \varnothing$，$1 \leqslant i \leqslant m$，

(c) $\bigcup_{i=1}^{m} S_i = A$。

称 S 是 A 的**覆盖**（covering）。若 S 还满足：

(d) $S_i \bigcap S_j = \varnothing$，$1 \leqslant i \neq j \leqslant m$。

称 S 是 A 的**划分**（partition）。

例如，$A = \{a,b,c\}$，则$\{\{a\},\{b\},\{c\}\}$、$\{\{a,b\},\{c\}\}$、$\{\{a,b,c\}\}$、$\{\{a,b\},\{b,c\}\}$都是 A 的覆盖，但前 3 个也是划分，$\{\{a,b\},\{b,c\}\}$不是划分。

[辨析]　一般称 S 为集合 A 的“分块”集合，规则(d)是指任意两个不同的分块不相交。

[辨析]　很明显，一个集合的划分一定是覆盖，是分块不相交的覆盖，而覆盖不一定是划分。

[定理 4-13]　若 $A = \{A_1, A_2, \cdots, A_m\}$和 $B = \{B_1, B_2, \cdots, B_n\}$是集合 X 的划分，则由所有 $A_i \bigcap B_j \neq \varnothing$ 构成的集合仍是 X 的划分，称为 A 和 B 的**交叉划分**。

证明　只要验证划分定义中的 4 条规则，且(b)已包含在假定中。

(a) 显然有 $A_i \bigcap B_j \subseteq X$。

(c) 对于所有 $A_i \bigcap B_j$，有

$$\bigcup_{i=1}^{m}\bigcup_{j=1}^{n}(A_i \cap B_j)=\bigcup_{i=1}^{m}(A_i \cap \bigcup_{j=1}^{n}B_j)=\bigcup_{i=1}^{m}(A_i \cap X)=\bigcup_{i=1}^{m}A_i = X。$$

除去空的分块并不影响最后的结果。因此，所有非空分块的并也为 X。

(d) 若 $A_i \cap B_j$ 和 $A_s \cap B_t$ 是两个不同的分块，则要么 $i \neq s$，$A_i \cap A_s = \varnothing$，要么 $j \neq t$，$B_j \cap B_t = \varnothing$。总之，$(A_i \cap B_j)\cap(A_s \cap B_t) = \varnothing$。故结论成立。

例如，$X=\{a,b,c\}$，$A=\{\{a\},\{b,c\}\}$，$B=\{\{a,b\},\{c\}\}$，则 A 和 B 的交叉划分为$\{\{a\},\{b\},\{c\}\}$。

[定义 4-15] 若 $A=\{A_1,A_2,\cdots,A_m\}$和 $B=\{B_1, B_2, \cdots, B_n\}$是集合 X 的划分，且每个 A 的分块都包含于 B 的某个分块，则称 A 是 B 的**加细划分**。

加细划分意味着分块更小。显然，交叉划分是原来两个划分的加细。

例 4-20 设 R 是集合 A 上的自反、对称和传递关系。若$\{A_1,A_2,\cdots,A_n\}$是 A 的子集集合，当 $i \neq j$ 时，$A_i \nsubseteq A_j$，使 a 和 b 在一个子集中当且仅当$<a,b>\in R$，求证$\{A_1,A_2,\cdots,A_n\}$是 A 的一个划分。

证明 (a) 由已知，所有 A_i 是 A 的子集。

(b) 对 $\forall i$，必有 $A_i \neq \varnothing$，否则与 $A_i \nsubseteq A_j$ 矛盾。

(c) 因所有 A_i 都是 A 的子集，故

$$\bigcup_{i=1}^{n}A_i \subseteq A。$$

对 $\forall a \in A$，因为 R 是自反的，有$<a,a>\in R$，故 a 在一个子集 A_i 中，有

$$A \subseteq \bigcup_{i=1}^{n}A_i。$$

所以，$\bigcup_{i=1}^{n}A_i = A$。

(d) 对 $\forall i \neq j$，若 $A_i \neq A_j$，必有 $A_i \cap A_j = \varnothing$。否则，有 $a \in A_i \cap A_j$。于是，对 $\forall x \in A_i$，$y \in A_j$，因 x 与 a、y 与 a 分别在一个子集中，有

$$<x,a>\in R \text{ 且 } <y,a>\in R。$$

又因为 R 是对称和传递的，有

$$<a,y>\in R \text{ 且 } <x,y>\in R。$$

这说明 x 与 y 属于同一子集，即 $x \in A_j$，有 $A_i \subseteq A_j$。与题目给定条件矛盾。结论成立。

4.5.2 相容与等价

[定义 4-16] 若集合 A 上的关系 R 是自反的和对称的，则称 R 是**相容关系**（compatibility relation）。如果 R 还具有传递性，则称 R 为**等价关系**（equivalence relation）。换言之，等价关系是具有传递性的相容关系。

假定 xRy。如果 R 为相容关系，称 x 与 y 是**相容的**，如果 R 为等价关系，称 x 与 y 是**等价的**，记作 $x \overset{R}{\sim} y$，或简记为 $x \sim y$。

例如，一群人组成的集合 A 上的“朋友”关系是相容关系，因为朋友关系是相互的，但不是等价关系，因为没有传递性。A 上的“肤色相同”关系是等价关系。一个年级若干学生集合上的“同班同学”关系也是等价关系。

例 4-21　设 m 为正整数，则整数集 $\mathbf{Z}$ 上的模 m 同余关系 $R=\{<x,y>|x\equiv y(\mathrm{mod}\,m)\}$ 是等价关系。

证明　R 的自反性和对称性是显然的。若 $<x,y>\in R$，$<y,z>\in R$，则 x 与 y 除以 m 的余数相同，y 与 z 除以 m 的余数相同。因此，x 与 z 除以 m 的余数相同，即 $<x,z>\in R$，故 R 是传递的。因此，R 是等价关系。结论成立。

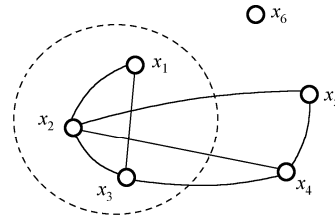
因为相容关系和等价关系都是自反和对称的，其关系图中每个元素都存在自环，且两个元素之间的连线是成对的。因此，约定不画出自环，且成对的连线用一条没有箭头的连线代替，以简化关系图。同时，由于关系矩阵中主对角线元素均为 1，且矩阵是对称的，故可以仅存储其下三角（或上三角）部分，从而达到节省存储空间的目的。

例如，$A=\{\text{cat, teacher, cold, desk, knife, by}\}$，定义关系 $R=\{<x,y>|x,y\in A$ 且 x 和 y 有相同的字母$\}$，则 R 是 A 上的相容关系。

记 $x_1=\text{cat}$, $x_2=\text{teacher}$, $x_3=\text{cold}$, $x_4=\text{desk}$, $x_5=\text{knife}$, $x_6=\text{by}$，则 R 的关系矩阵和关系图可简化为图 4-7。

x_2	1				
x_3	1	1			
x_4	0	1	1		
x_5	0	1	0	1	
x_6	0	0	0	0	0

(a) 关系矩阵



(b) 关系图

图 4-7

4.5.3　相容关系产生的完全覆盖

1．相容类与最大相容类

[定义 4-17] 设 R 是集合 A 上的相容关系，$C\subseteq A$。若 C 中的任意两个元素 x 和 y 都有关系 R，则称 C 是由 R 产生的**相容类**（compatibility class）。

例如，前例中的$\{x_1\}$、$\{x_1,x_2\}$、$\{x_1,x_3\}$、$\{x_2,x_3\}$、$\{x_6\}$、$\{x_2,x_4,x_5\}$都是相容类，但前 4 个可以通过添加其他元素构成更大的相容类，后 2 个不能再扩大。因为 R 存在自反性，故任何元素 $x\in A$ 自己组成的子集$\{x\}$都是一个相容类。

[定义 4-18] 设 R 是集合 A 上的相容关系，由 R 产生的不能真包含（严格包含）在任何其他相容类中的相容类称为**最大相容类**，记作 C_R。

在相容关系图中，一个子集与其结点之间的连线构成的图称为“子图”，而任意两个结点之间都有连线的子图称为“完全子图”。显然，任何一个完全子图都是一个相容类。当一个完全子图的结点不能再增加时，其结点集合就是最大相容类。例如，对于图 4-7 的相容关系 R，可以找出其所有的最大相容类：

$\{x_1,x_2,x_3\}$，$\{x_2,x_3,x_4\}$，$\{x_2,x_4,x_5\}$，$\{x_6\}$。

[定理 4-14] 若 C 是一个相容类，则存在一个最大相容类 C_R，使 $C \subseteq C_R$。

对于有限集，在保证与已有相容类中所有元素都相容的情况下，逐个添加元素，有限步即可找到最大相容类。

2．完全覆盖

[定义 4-19] 设 R 是集合 A 上的相容关系，由其最大相容类构成的集合称为 A 的**完全覆盖**。记作 $C_R(A)$。

事实上，因为任一元素 $a \in A$ 自己组成的子集$\{a\}$是一个相容类，由定理，必包含在一个最大相容类中，故 $A \subseteq \bigcup C_R$。$\bigcup C_R \subseteq A$ 是显然的，说明最大相容类集合确是 A 的覆盖。

例如，对图 4-7 的关系 R，$\{\{x_1,x_2,x_3\}$，$\{x_2,x_3,x_4\}$，$\{x_2,x_4,x_5\}$，$\{x_6\}\}$构成了 A 的完全覆盖。

[辨析] 由一个相容关系可以生成多个相容类，也可以构成集合 A 的多个覆盖，但完全覆盖只有一个。

4.5.4 等价关系产生的划分

1．等价类

[定义 4-20] 设 R 是集合 A 上的等价关系，对任意的 $a \in A$，称下述集合为由元素 a 生成的 R 等价类，简称为 a 的**等价类**（equivalence class）。

$$[a]_R = \{x \mid x \in A \wedge < a,x > \in R\}。$$

如果 $b \in [a]_R$，称 b 为等价类的**代表元**。在不至于混淆时，$[a]_R$ 可简记为$[a]$。

因为 aRa，因此，$a \in [a]_R$，可见任何等价类都是非空的，即 $[a]_R \neq \varnothing$。

[辨析] 元素 a 生成的等价类是由所有与 a 等价的元素组成的集合，故可记为：

$$[a]_R = \{x \mid x \in A \wedge a \sim x\}。$$

因为等价关系是对称的，故还可记为：

$$[a]_R = \{x \mid x \in A \wedge xRa\} = \{x \mid x \in A \wedge x \sim a\}。$$

[理解] 符号 $[a]_R$ 表明此对象与 a 和 R 有关，受 a 和 R 影响，可视为以 a 和 R 为参数的函数，函数值为集合。如果将集合 A 也视为参数，甚至可表示为 $[a]_R^A$ 或 $[a]_R(A)$，这是数学描述中常用的技巧。

例如，对于前文提到的一个年级学生集合上的“同班同学”关系，任意指定一名学生 s，其所在班级的所有同学都与 s 等价，因此，s 生成的等价类就是其班级所有学生的集合。

设 A 是一个字符串集合，定义 A 上的关系 R=$\{<x, y> \mid x$ 与 y 的前 31 个字符相同$\}$。显然 R 是等价关系。很多 C 语言的编译器按此关系处理变量名（实体名），所有等价的字符串构成等价类，彼此被认为是相同的标识符。

对于整数集合上的模 3 同余关系，共有如下 3 个不同的等价类：

$[0]_R=\{\cdots,-6,-3,0,3,6,\cdots\}$，$[1]_R=\{\cdots,-5,-2,1,4,7,\cdots\}$，$[2]_R=\{\cdots,-4,-1,2,5,8,\cdots\}$。

一般地，模 m 同余关系所产生的等价类也称为“同余类”或“剩余类”。模 m 同余关系共有 m 个不同的同余类$[0]_R$，$[1]_R$，$[2]_R$，…，$[m-1]_R$。

因为等价是相互的，故$[a]_R$是 a 生成的，也是该集合中任何一个元素生成的。换言之，一个等价类是由相互等价的元素构成的集合，其中任何一个都是代表元素，都可以生成该等价类。

[定理 4-15] 设 R 是集合 A 上的等价关系，对任意的 a，$b\in A$，下述 3 个命题等价：

(1) $<a,b>\in R$。　　(2) $[a]_R=[b]_R$。

(3) $[a]_R\cap[b]_R\neq\varnothing$。

证明　采用循环等价法。

(1)⊢(2)。对 $\forall x\in[a]_R$，有 $<x,a>\in R$。再由$<a,b>\in R$和传递性，有 $<x,b>\in R$，知 $x\in[b]_R$，故 $[a]_R\subseteq[b]_R$。

同理，$[b]_R\subseteq[a]_R$。故 $[a]_R=[b]_R$。

(2)⊢(3)。因 $[a]_R=[b]_R$，显然有 $[a]_R\cap[b]_R=[a]_R\neq\varnothing$。

(3)⊢(1)。因 $[a]_R\cap[b]_R\neq\varnothing$，存在 $t\in[a]_R\cap[b]_R$，有

$$t\in[a]_R\wedge t\in[b]_R\Rightarrow<a,t>\in R\wedge<t,b>\in R。$$

因为 R 是传递的，故 $<a,b>\in R$。

2．商集

[定义 4-21] 若 R 是集合 A 上的等价关系，则其等价类集合$\{[a]_R\mid a\in R\}$称为 A 关于 R 的**商集**，记作 A/R。

例如，对于模 3 同余关系，有 $\mathbf{Z}/R=\{[0]_R,[1]_R,[2]_R\}$。

[定理 4-16] 由 A 上的等价关系 R 确定的商集 A/R 构成了 A 的一个划分，称为 R **诱导的划分**。

证明　显然，划分定义中的(a)、(b)和(d)均成立，只要说明$\bigcup_{a\in A}[a]_R=A$。

对任意的 $x\in A$，因为自反性，有 xRx，即 $x\in[x]_R$，故 $x\in\bigcup_{a\in A}[a]_R$，说明 $A\subseteq\bigcup_{a\in A}[a]_R$。

因为$\bigcup_{a\in A}[a]_R\subseteq A$是自然存在的，所以$\bigcup_{a\in A}[a]_R=A$。结论成立。

利用一个等价关系将集合划分为商集是很有价值的。例如，将所有人的集合利用“肤色相同”关系得到的商集为{白人集合，黄种人集合，黑人集合}，因为同色人是等价的。需要了解不同人种的特点时，只要从每个人种集合中任意找出一人作为代表元即可。这也体现了“物以类聚，人以群分”的道理。

[辨析] 为什么叫做商集？形象地看，等价类集合$\bigcup_{a\in A}[a]_R$就是 A 被 R 除所得的商 A/R。

4.5.5　由覆盖、划分生成相容关系和等价关系

由一个集合上的覆盖和划分也能得到对应的相容关系和等价关系。

[定理 4-17] 给定集合 A 的子集集合 $S=\{A_1,A_2,\cdots,A_m\}$，由 S 构造如下关系：

$$R=\bigcup_{i=1}^{m}A_i\times A_i。$$

若 S 是 A 的覆盖，则 R 是 A 上的相容关系。若 S 是 A 的划分，则 R 是 A 上的等价关系。

证明 (1) S 是 A 的覆盖$\vdash R$ 是相容关系。

(a) 自反性。对任意的 $a \in A$，有 k，使 $a \in A_k$，所以 $< a,a > \in A_k \times A_k$，即 aRa。

(b) 对称性。若 aRb，有 k，使 $< a,b > \in A_k \times A_k$，所以 $< b,a > \in A_k \times A_k$，即 bRa。

(2) S 为 A 的划分$\vdash R$ 是等价关系。只需要证明传递性。若 aRb 且 bRc，因分块不相交，必有 k，使 a，b，$c \in A_k$。因此，$< a,c > \in A_k \times A_k$，即 aRc。故 R 为 A 上的等价关系。

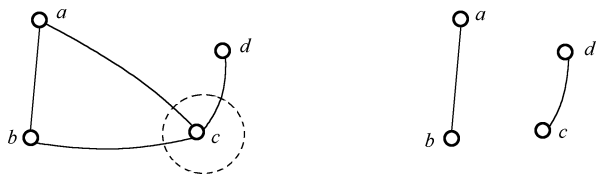
此定理是构造性的，说明了如何由子集集合来构造相容关系或等价关系。

例如，有 $A = \{a,b,c,d\}$ 的子集集合 $\{\{a\},\{a,b,c\},\{c,d\}\}$、$\{\{a,b\},\{c,d\}\}$，由定义生成的关系 R_1 和 R_2 为：

$$\begin{aligned} R_1 &= \{\{a\}\times\{a\} \cup \{a,b,c\}\times\{a,b,c\} \cup \{c,d\}\times\{c,d\}\} \\ &= I_A \cup \{< a,b >,< a,c >,< b,a >,< b,c >,< c,a >,< c,b >,< c,d >,< d,c >\}, \\ R_2 &= \{\{a,b\}\times\{a,b\} \cup \{c,d\}\times\{c,d\}\} \\ &= I_A \cup \{< a,b >,< b,a >,< c,d >,< d,c >\}。 \end{aligned}$$

显然，R_1 是相容关系，R_2 为等价关系。

为什么在 S 是覆盖或划分时会导致关系 R 的性质不同呢？其原因在于子集是否相交。



(a)覆盖　　(b)划分

图 4-8

图 4-8 分别是 R_1 和 R_2 的关系图。由于覆盖中分块存在着交集$\{c\}$，导致两块间的元素 a 和 d 通过 c 相连，但关系中不存在序偶$<a,d>$，传递性被破坏。而在划分产生的关系中，各块都是“局部的全关系”，本身已在块内具有传递性，也不可能通过分块之间的公共元素形成“通路”，故经过子集合并后传递性仍被维持下来。

[辨析] 集合的划分与等价关系之间存在一一对应，但覆盖与相容关系之间不是一一对应的。

[延伸] 划分、覆盖及等价关系不仅在日常生活中常用，它们与分类、聚类、数据分析和数据挖掘也有着紧密的关联。另外，可以将普通集合推广到模糊集合，在此基础上建立模糊关系和模糊等价关系，进而解决具有模糊性的聚类分析问题[24–27]。

思考与练习 4.5

4-38　覆盖与划分有何异同？相容关系与等价关系有何异同？

4-39　何谓相容类和最大相容类？何谓等价类？按等价类的方式定义相容类是否可行，为什么？

4-40　找出集合 $A=\{a,b,c,d\}$ 的所有划分，并说明集合上可以定义多少个等价关系。

4-41　设 π_1 和 π_2 是集合 $A\neq\varnothing$ 上的划分，说明下述集合是否为 A 的划分。

(a) $\pi_1\cap\pi_2$。　　(b) $\pi_1\cup\pi_2$。

(c) $\pi_1-\pi_2$。

4-42　设 R 是集合 X 上的二元关系，证明 $I_X\cup R\cup R^{-1}$ 是 X 上的相容关系。

4-43　设集合 $X=\{x_1,x_2,\cdots,x_6\}$ 上的相容关系 R 具有如下的简化关系矩阵：

$$\begin{array}{cccccc} x_2 & 1 & & & & \\ x_3 & 1 & 1 & & & \\ x_4 & 0 & 1 & 1 & & \\ x_5 & 0 & 1 & 0 & 1 & \\ x_6 & 0 & 0 & 0 & 0 & 0 \\ & x_1 & x_2 & x_3 & x_4 & x_5 \end{array}$$

求出 R 确定的 X 的完全覆盖。

4-44　设 $C=\{S_1,S_2,\cdots,S_m\}$ 是集合 A 的覆盖，求由此覆盖确定的 A 上的相容关系并说明，在什么条件下，此覆盖确定的关系为等价关系？

4-45　设 α 和 β 是集合 X 上的相容关系，证明或否定：

(a) $\alpha\cap\beta$ 是 X 上的相容关系。　　(b) $\alpha\cup\beta$ 是 X 上的相容关系。

(c) $\alpha\circ\beta$ 是 X 上的相容关系。

4-46　设 α 和 β 是集合 X 上的等价关系，证明或否定：

(a) $\alpha\cap\beta$ 是 X 上的等价关系。　　(b) $\alpha\cup\beta$ 是 X 上的等价关系。

(c) $\alpha\circ\beta$ 是 X 上的等价关系。

4-47　设 $S=\{1,2,3,4,5\}$，确定 S 上的一个等价关系 R，使之产生的商集 S/R 为 $\{\{1,2\},\{3\},\{4,5\}\}$。

4-48　设 R 是集合 X 上的等价关系，定义

$$S=\{<a,b>\mid \exists x(x\in X\wedge aRx\wedge xRb)\}。$$

证明 S 是等价关系。

4-49　设 R 是集合 X 上的等价关系，证明 R^2 也是等价关系。

4-50　设有定义在 $\mathbf{Z}^+\times\mathbf{Z}^+$ 上的下列关系 R，判断其是否为等价关系？证明你的结论。

(a) $R=\{<<a,b>,<c,d>>\mid a+d=b+c\}$。

(b) $R=\{<<a,b>,<c,d>>\mid a+c=b+d\}$。

4-51　设 α 和 β 分别是集合 X 和 Y 上的等价关系，定义关系 $R=\{<<a,b>,<c,d>>\mid <a,c>\in\alpha\wedge<b,d>\in\beta\}$，证明 R 是 $X\times Y$ 上的等价关系。

4-52　设 R 是集合 A 上的对称和传递关系，且命题 $\forall a(a\in A\rightarrow\exists b(b\in A\wedge<a,b>\in R))$ 成立，证明 R 是等价关系。

4-53　设 α 和 β 是非空集合 A 上的等价关系，判断下述关系是否为等价关系，证明你的结论。

(a) $(A\times A)-\alpha$。　　(b) $\alpha-\beta$。

(c) $r(\alpha-\beta)$。

4.6 序 关 系

“序”是数据集的一种十分重要的性质，也是数据集可被广泛应用的根本原因，因为利用序关系可以将数据集的元素按需要进行适当排列。事实上，计算机工作的很大一部分时间都花在与序有关的数据处理上。

4.6.1 体现部分次序的偏序关系

任意整数集合，如 **N**，显然可以依赖“≤”关系对元素进行排序，即≤是一种序关系。根据关系性质可知，≤具有自反性、反对称性和传递性，这就是使关系能够反映出次序的最低要求。

[定义 4-22] 若集合 A 上的关系 R 是自反的、反对称的和传递的，则称 R 是**偏序关系**（partial ordering relation）。普通的偏序关系多记作≼，$<x,y>\in\preccurlyeq$通常记作更直观的 $x\preccurlyeq y$，且称序偶$<A,\preccurlyeq>$为**偏序集**（partial ordering set，poset）。

例如，实数集、整数集上的小于等于关系≤、大于等于关系≥是偏序关系；一个正整数集合上的整除关系|是偏序关系；一个集合 A 的幂集 $\mathscr{P}(A)$ 上的包含关系 $\subseteq$ 是偏序关系。但实数集上的>和<都不是偏序关系，它们无自反性，即对于一个实数 a，$a>a$ 和 $a<a$ 均不成立。

[定义 4-23] 设$<A,\preccurlyeq>$为偏序集，对于 a，$b\in A$，如有 $a\preccurlyeq b$ 或 $b\preccurlyeq a$，则称 a、b 是可比的，否则为不可比的。

[辨析] “偏”意为“不全”或“部分”而非“不正”，偏序就是部分序，故也称为“半序”。这意味着一个偏序集中并非任意两个元素都有关系，没有关系也就意味着二者是不可比的。例如，对于整除关系，2 与 3 是不可比的，无法判定二者的“大小”。

[定义 4-24] 如果 $a\preccurlyeq b$ 且 $a\neq b$，则称为 a 小于 b，记作 $a\prec b$。

以上两个定义仅是对两个元素之间的关系做一种简单的描述，以方便叙述。

4.6.2 哈斯图

与相容关系类似，偏序关系的关系图也可以简约画出。因为自反性，每个元素均有自环，可以省略不画，且任何两点之间至多只有一个方向的连线，当约定方向后就可以省略箭头。更完整的简化图称为**哈斯图**（或**哈塞图**，Hasse 图），它是以德国数学家 Helmut Hasse 名字命名的。

[定义 4-25] 在偏序集$<A,\preccurlyeq>$中，对任意的 x，$y\in A$，如果 $x\prec y$，且 A 中不存在 z 满足 $x\prec z$，$z\prec y$，则称 y **盖住**（cover）了 x，且称下述集合为**盖住集**。

$$COV(A)=\{<x,y>|x,\ y\in A \text{ 且 } y \text{ 盖住 } x\}。$$

盖住集是由所有具有盖住关系的序偶组成的集合。

[辨析] “y 盖住了 x”是指 $x\prec y$ 且二者中间不能插入其他元素。

例如，图 4-9 所示为集合 $A=\{1,2,3\}$上偏序关系≼$=\{<1,1>,\ <2,2>,\ <3,3>,\ <1,3>,$

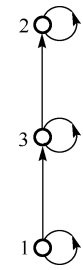


图 4-9

<1,2>, <3,2>}的关系图，元素之间的“大小”关系是 $1 \prec 3$，$3 \prec 2$。因此，3 盖住 1，2 盖住 3，但 2 不能盖住 1，因为它们之间存在着与 2 和 1 都有关系的元素 3。

例 4-22　设 A 是整数 12 的因子集合，求 A 上整除关系|的盖住集 $COV(A)$。

解　$A=\{1,2,3,4,6,12\}$，有

$|=I_A \cup \{<1,2>,<1,3>,<1,4>,<1,6>,<1,12>,<2,4>,<2,6>,<2,12>,<3,6>,<3,12>,<4,12>,<6,12>\}$。

于是，有

$$COV(A)=\{<1,2><1,3>,<2,4>,<2,6>,<3,6>,<4,12>,<6,12>\}。$$

根据盖住集，可按下述方式绘出哈斯图：

(a) 用小圆圈表示元素；

(b) 如果 $a \prec b$，则元素 b 置于元素 a 的上方（隐含了由下至上的连线方向）；

(c) 若 $<a,b> \in COV(A)$，在 a 和 b 之间有一条连线。

例如，图 4-10 给出了上述整除关系的哈斯图。

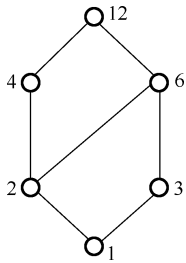


图 4-10

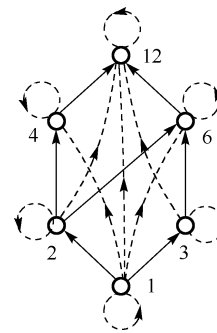


图 4-11

为什么偏序关系的关系图可以简化为哈斯图？观察图 4-11 中未经简化的关系图会发现，只要按“由小到大”的层次绘制关系图，因为传递性的存在，那些“跨元素”的边一定会出现，使图在不计方向时构成了若干闭合的“回路”，或者说两个结点之间存在着多于一条“可到达的路”。删除这些多余的跨元素边也就消除了回路（包括因自反性形成的自回路），其结果就是哈斯图。

[理解] 在根据哈斯图写出偏序关系时，一定要注意自反性和传递性。

例 4-23　设 $A_1=\{a,b\}$，$A_2=\{a,b,c\}$，画出 $\mathscr{P}(A_1)$和 $\mathscr{P}(A_2)$上集合包含关系 $\subseteq$ 的哈斯图。

解　$\mathscr{P}(A_1)=\{\varnothing,\{a\},\{b\},A\}$，$\mathscr{P}(A_2)=\{\varnothing,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},A\}$。于是有：

$COV(A_1)=\{<\varnothing,\{a\}>,<\varnothing,\{b\}>,<\{a\},\{a,b\}>,<\{b\},\{a,b\}>\}$，

$COV(A_2)=\{<\varnothing,\{a\}>,<\varnothing,\{b\}>,<\varnothing,\{c\}>,<\{a\},\{a,b\}>,<\{b\},\{a,b\}>,<\{a\},\{a,c\}>,<\{b\},\{b,c\}>,<\{c\},\{a,c\}>,<\{c\},\{b,c\}>,<\{a,b\},\{a,b,c\}>,<\{a,c\},\{a,b,c\}>,<\{b,c\},\{a,b,c\}>\}$。

如图 4-12 所示为这两个关系的哈斯图。

[延伸] 可以找到多种计算哈斯图的方法，它们的计算量并不相同，选择一种适当的算法并用计算机语言实现是一种很好的训练，也可以直接应用在解决一些实际问题中[28,29]。

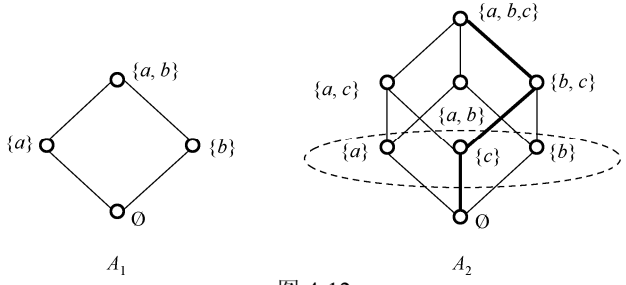


图 4-12

4.6.3 链与全序关系

利用哈斯图可以清楚地看出元素之间的关系。

[定义 4-26] 设<A, ≤>是一个偏序集，$C \subseteq A$，$C \neq \varnothing$。若 C 中任意两个元素都有关系，即二者是可比的，则称 C 为**链**（chain）。若 C 中任意两个元素都没有关系，即二者不可比，称 C 为**反链**（anti-chain）。约定：只含有一个元素的子集既是链也是反链。

例如，A 为单位员工集合，≤表示上下级关系，则{总经理，部门经理，职工甲}构成链，而{职工甲，职工乙，职工丙}构成反链。

在哈斯图中，从任何一元素开始，沿一条线路由下到上“走过的路”是一个链，如图 4-12 中的粗实线部分的元素构成的子集。没有两个元素处于同一条路上的元素构成反链，如图 4-12 中的虚线椭圆形区域内的元素构成的子集{{a},{b},{c}}。

[辨析] 一个子集不是链并不意味着它就是反链，反之亦然。

[定义 4-27] 设<A, ≤>是一个偏序集。若 A 本身是一个链，则称<A, ≤>为**全序集**（total order set）或**线序集**（linear order set），而≤称为**全序关系**或**线序关系**。

简单讲，全序就是指全都有序，即此关系的哈斯图是“一个链”或“一条线”。因此，任意两元素都是可比的。

例如，整数集 **Z** 上的≤关系，集合 $A=\{\varnothing,\{a\},\{a,b\},\{a,b,c\}\}$ 上的 $\subseteq$ 关系都是全序关系，其哈斯图如图 4-13 所示。

例 4-24 找出集合{0,1,2,3}上包含序偶<0,3>和<2,1>的线序关系。

解 这里只要求满足 0≤3 和 2≤1，故可以有多种可能。图 4-14 说明了可能构成的 6 种线序关系的哈斯图。

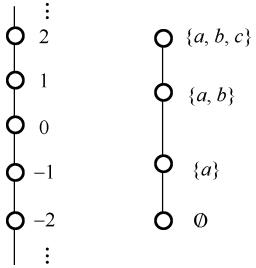


图 4-13

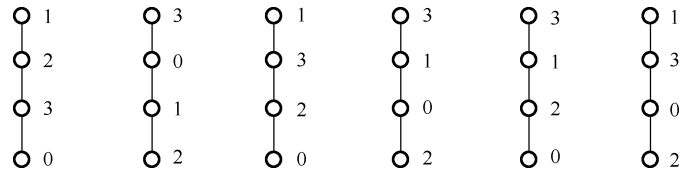


图 4-14

其中，第一个线序关系为{<0,0>,<1,1>,<2,2>,<3,3>,<0,3>,<0,2>,<0,1>,<3,2>,<3,1>,<2,1>}，其他线序关系可类似写出，应注意反映出自反性和传递性。

4.6.4　偏序集的特殊元素

“序”可以使我们能比较两个元素的大小，进而可以在包含若干元素的集合中找出一些特殊的元素。

1．极大元和极小元

[定义 4-28] 设$<A, \preccurlyeq>$是一个偏序集，$B \subseteq A$。若$b \in B$，且没有$x \in B$使得$b \prec x$，则称b是B的**极大元**（maximal element）。同理，若没有$x \in B$使得$x \prec b$，则称b是B的**极小元**（minimal element）。

注意极大元和极小元（或称极大元素和极小元素）都在子集B中讨论。

[辨析] 极大元类似在局部范围内“没有比它更高的山”，但不保证它比其他元素都大，这是因为可能有相等的或不可比的元素。极小元则类似在局部“没有比它更低的谷”。

例如，观察图 4-15 所示哈斯图中的子集$B = \{3,4,5,6\}$。B的极大元为 4 和 6，极小元为 3 和 5。显然，一个子集的极大元和极小元都可能不是唯一的。

[辨析] 不要误认为 1 一定小于 3，4 一定小于 5。在这个偏序关系中，$1 \preccurlyeq 2$，$3 \preccurlyeq 2$，$5 \preccurlyeq 4$，1 与 3~6 都是不可比的。尽管 4 和 6 在图中的位置比 1 高，但它们不在一个链上，没有大小关系。

2．最大元和最小元

[定义 4-29] 设$<A, \preccurlyeq>$是一个偏序集，$B \subseteq A$。若$b \in B$，且对所有的$x \in B$，都有$x \preccurlyeq b$，则称b是B的**最大元**（greatest element）。若对所有的$x \in B$，都有$b \preccurlyeq x$，则称b是B的**最小元**（least element）。

[辨析] 最大元和最小元（或称最大元素和最小元素）也都在子集B中讨论。通俗地说，最大元要大于等于子集中的所有元素，最小元要小于等于子集中的所有元素。

例如，图 4-15 中的子集B既无最大元也无最小元。子集$C = \{1,2,3\}$存在最大元 2，但不存在最小元。子集$D = \{4,5,6\}$存在最小元 5，但不存在最大元。

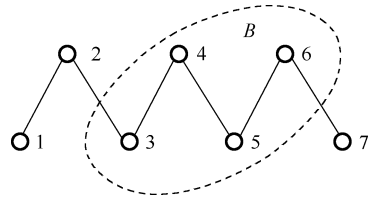


图 4-15

[定理 4-18] 若一个子集中最大元（最小元）存在，则必定是唯一的。

证明　只说明最大元。

若a和b都是最大元。由a是最大元，有$b \preccurlyeq a$。又由b是最大元，有$a \preccurlyeq b$。由反对称性知，$a=b$。结论成立。

3．子集的界

[定义 4-30] 设$<A, \preccurlyeq>$是一个偏序集，$B \subseteq A$。若$a \in A$，且对所有的$x \in B$，都有$x \preccurlyeq a$，则称a是B的**上界**。若对所有的$x \in B$，都有$a \preccurlyeq x$，则称a是B的**下界**。

若B存在最小的上界，称其为**上确界**（LUB，least upper bound）。若B存在最大的下界，称其为**下确界**（GLB，greatest lower bound）。

[辨析] “界”并不要求一定在子集 B 中，可以在整个 A 内讨论。不严格说，界是扩大了范围的最大元和最小元。很明显，B 的最大元一定是上界和上确界，B 的最小元一定是下界和下确界。

与最大和最小元类似，上确界和下确界不一定存在，但若存在必是唯一的。

图 4-16 说明了这些特殊元素的存在范围。

例 4-25 设有图 4-17 所示的偏序关系的哈斯图，找出子集 $B=\{c,d,e,f\}$、$C=\{c,e,f\}$、$D=\{c,d,e\}$ 的极大元、极小元、最大元、最小元、上界、下界、上确界和下确界。

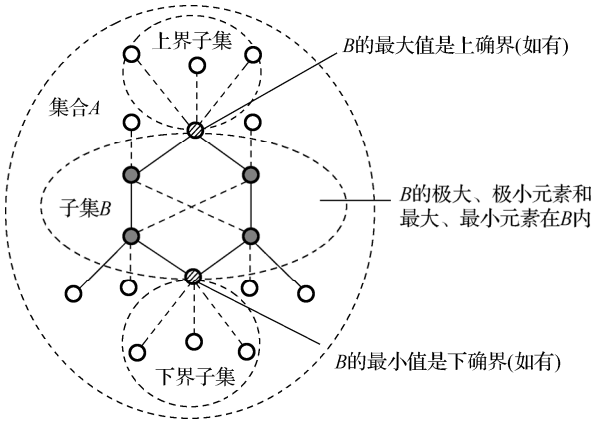


图 4-16

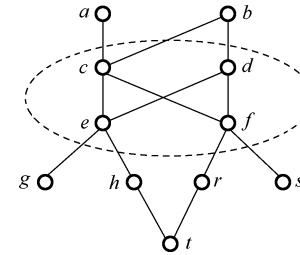


图 4-17

解 B 的极大元为 c 和 d，极小元为 e 和 f，无最大元和最小元，上界和上确界为 b，下界和下确界为 t。

C 的极大元为 c，极小元为 e 和 f，最大元为 c，无最小元，上界为 a、b 和 c，上确界为 c，下界和下确界为 t。

D 的极大元为 c 和 d，极小元为 e，无最大元，最小元为 e，上界、上确界为 b，下界为 e、g、h 和 t，下确界为 e。

例 4-26 构造一个非空线序集，其中某些子集没有最小元。

解 由于线序集的所有元素都是可比的。因此，有限的线序集总能找到最小元。换言之，应该构造一个无限的线序集才能满足要求。

例如，整数集 $\mathbf{Z}$ 上的≤关系构成线序关系，但 $\mathbf{Z}$ 本身、偶数集、奇数集都没有最小元。又如，区间(0,1)内的所有实数上的≤关系构成线序关系，该集合及其子集$\{1/n \mid n\in\mathbf{Z}^+\}$都没有最小元。当然，区间(0,1)内的所有实数组成的集合也没有最大元。

思考与练习 4.6

4-54 ≤是集合 A 上的偏序关系的含义是什么？

4-55 若≤是集合 A 上的偏序关系，对于元素 $x,y\in A$，x 盖住 y 是什么意思？

4-56　找出下述偏序集中的不可比元素。

(a) $<\mathscr{P}(\{0,1,2\}), \subseteq>$。　　(b) $<\{1,2,4,6,8\}, |>$。

4-57　设集合 X 分别为 {3,5,15}、{1,2,3,6,12}、{3,9,27,108}、{1,2,3,6,12,24,36,48}、{1,2,3,5,7,11,13}、{3,5,9,15,24,45}，画出 X 上的整除关系的哈斯图，并说明哪些是全序关系。

4-58　设 A 为集合，$B = \mathscr{P}(A) - \{\varnothing\} - \{A\} \neq \varnothing$。求偏序集 $<B, \subseteq>$ 的极大元、极小元和最小元。

4-59　构造下述偏序集的例子。

(a) 一个偏序集，不是线序集，其中某些子集没有最大元素。

(b) 一个偏序集，它的某些子集没有最小元素，但存在下确界。

(c) 一个偏序集，它的某些子集存在上界，但没有上确界。

4-60　证明如果偏序集的一个子集存在最小元素，则恰好存在唯一的最小元素。

4-61　证明如果偏序集的一个子集存在上确界，则恰好存在唯一的上确界。

4-62　对于图 4-18 所示的哈斯图表示的偏序关系，求出下述元素。

(a) 极大、极小元素。

(b) 最大、最小元素。

(c) 子集{a,b,c}的上界和上确界。

(d) 子集{j,k,h}的下界和下确界。

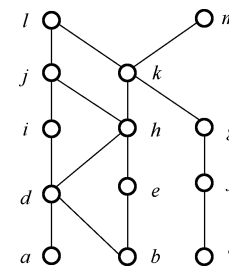


图 4-18

4-63　设集合 $X = \{a, b, c, d, e\}$，X 上偏序集 $R = \{<d,b>, <d,c>, <d,a>, <b,a>, <c,a>, <e,c>, <e,a>\} \cup I_X$，找出 X 的最大元素、最小元素、极大元素和极小元素，再找出子集 $\{a,b,c\}$、$\{b,c,d\}$ 和 $\{c,d,e\}$ 的上界、下界、上确界和下确界。

4-64　画出图 4-19 所示的集合{1,2,3,4}上的 4 个偏序关系的哈斯图，并指出其中的全序关系。

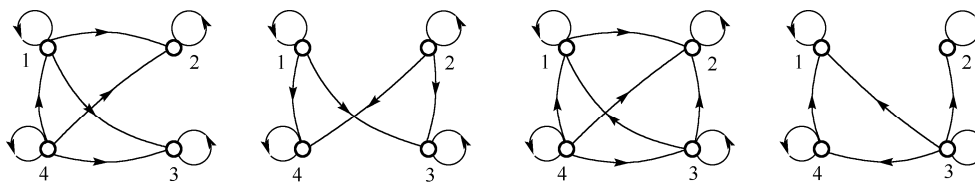


图 4-19

第 5 章 函 数

函数是一个基本的数学概念，应用十分广泛，体现在所有与数学和计算机相关的课程里。在数学上，函数 $y=f(x)$ 用于建立实数集上两个量之间的对应关系。在程序设计语言中，函数被用来计算值或执行某些操作。这里将函数视为一类特殊的二元关系来讨论。

5.1 从关系到函数

5.1.1 函数的概念

[定义 5-1] 若 f 是集合 X 到 Y 的关系，且对于每个 $x\in X$，有唯一的 $y\in Y$，使得 $<x,y>\in f$，则称 f 是 X 到 Y 的**函数**（function）或**映射**（mapping）。记作

$$f:\ X\to Y \text{ 或 } X\xrightarrow{f}Y \text{ 。}$$

也可记作 $f\in Y^X$ 。

函数还称为映照或对应等，映射的称呼更能揭示其内涵，参见图 5-1。在一般关系中，x 与 y 有关系记作 $<x,y>\in f$ 或 xfy，但在函数中一般记作 $y=f(x)$，称 x 为**自变量**，称其取值范围为**定义域**（domain）；y 是 x 的函数值，称为**因变量**，称其取值范围为**值域**（range）。同时，称 y 为 x 在 f 作用下的**像**（image），x 为 y 的**原像**（inverse image）。

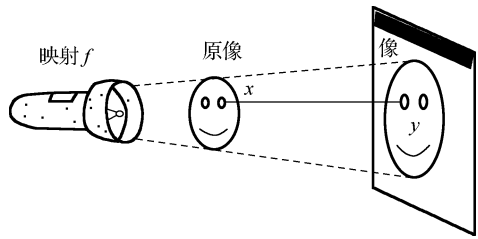


图 5-1

函数与一般关系有两个重要区别，它们是判断一个关系是否为函数的依据：

(1) 函数的定义域必须是 X 而不能是 X 的子集，即 $\mathrm{dom}\, f=X$。

(2) 一个自变量只能有唯一的函数值，即像。符号描述为：

$$\forall x((x\in X\wedge f(x)=y\wedge f(x)=z)\to y=z)\text{ 。}$$

这一要求体现了函数的单值性。

[辨析] 函数的定义域充满和单值性要求保证了在定义域内可以画出一条简单函数曲线，这种直观认识有助于记住函数的定义，也不至于将函数的单值性与后文的单射混淆。

难以形容函数应用的广泛程度。例如，在生活、生产或是科学研究中，“分类”是一项频繁的工作，可以这样描述：

对一组类别 $C=\{y_1,y_2,\cdots,y_n\}$和一组待分类的项目集合 $I=\{x_1,x_2,\cdots,x_m\}$，确定一个映射 f：$I\to C$，其含义是为每个项 $x_i\in I$ 唯一确定一个类别 $y_j\in C$，使 $f(x_i)=y_j$，故将 f 称为“分类器”。

很明显，这里的 f 是映射而非普通关系的原因是，每个项目都需要确定唯一的类别。

[辨析] 既然函数是关系，故仍是一个序偶的集合。

在函数 f：$X\to Y$ 中，f 的值域 $\mathrm{ran}\,f=Y$，但所有 x 的像一般仅是 Y 的子集，称为**像集**，记作

$$R_f=f(X)=\{f(x)|x\in X\}=\{y\mid\exists x(x\in X\wedge y=f(x))\}。$$

一些函数可以用解析表达式表示，如：

$$f\text{：}\ \mathbf{R}\to\mathbf{R}，\quad y=f(x)=2x^2+1。$$

又如，若 A 是全集 U 的子集，定义函数：

$$\mu_A\text{：}\ U\to\{0,1\}，\quad \mu_A(x)=\begin{cases}1 & ,x\in A\\ 0 & ,x\notin A\end{cases}。$$

这样的函数 μ_A 称为集合 A 的特征函数。

由于函数是一种关系，故也可以利用普通关系的序偶集合方式表示函数。

例 5-1　判断下述关系是否构成函数。

(1) $f=\{<x_1,x_2>\mid x_1,x_2\in\mathbf{N}\text{且}x_1+x_2<10\}$。

(2) $f=\{<y_1,y_2>\mid y_1,y_2\in\mathbf{R}\text{且}y_2=y_1^2\}$。

(3) $f=\{<y_1,y_2>\mid y_1,y_2\in\mathbf{R}\text{且}y_1=y_2^2\}$。

(4) $f=\{<x_1,x_2>\mid x_1,x_2\in\mathbf{N}\text{且}x_2=\text{小于}x_1\text{的素数个数}\}$。

解　(1) 否。若 $x_1\geqslant 10$ 则没有像，若 $x_1<10$ 则可以有多个像。

(2) 是。这里的函数就是 $y=f(x)=x^2$。

(3) 否。因为 $y_1<0$ 时没有像，而 $y_1>0$ 时有 2 个像 $\sqrt{y_1}$ 和 $-\sqrt{y_1}$，像不唯一。

(4) 是。对于自然数 x_1，小于 x_1 的素数个数或者为 0，或者为某个正整数。

如果一个函数 f：$X\to Y$ 的定义域 X 为多元组集合，则 f 就是一个多元函数。

5.1.2　函数集

[定义 5-2] 设函数 $f:X\to Y,g:U\to V$。若 $X=U$，$Y=V$ 且对于任意的 $x\in X$，都有 $f(x)=g(x)$，则称 f 与 g 相等，记作 $f=g$。

简言之，两函数相等是指它们的定义域相同、值域相同且对应关系相同。这被称为函数相等的“三要素”，由此来判定不同形式的函数是否为同一个。

若 $|X|=m$，$|Y|=n$。虽然 $X\times Y$ 的子集都是关系，有 2^{mn} 个，但并不都是函数。显然，对于每

个 $x \in X$，它的像可以是 Y 中的任意一个元素，有 n 种可能，故 m 个元素的像共有 n^m 种可能。

[定义 5-3] X 到 Y 的所有函数组成的集合称为**函数集**，记作 Y^X，符号表示为：

$$Y^X = \{f | f: X \to Y\}。$$

若 $|X| = m$，$|Y| = n$，则 X 到 Y 的函数共 n^m 个。

[辨析] 为什么将 X 到 Y 的函数集记作 Y^X 而不是 X^Y？因为 $|Y^X| = |Y|^{|X|} \neq |X|^{|Y|}$。

例 5-2 设 $A = \{1,2,3\}$，$B = \{a,b\}$，求 B^A。

解 B^A 共有 $2^3 = 8$ 个函数，可记作 $B^A = \{f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7\}$，且

$$f_0 = \{<1,a>,<2,a>,<3,a>\},\quad f_1 = \{<1,a>,<2,a>,<3,b>\},$$
$$f_2 = \{<1,a>,<2,b>,<3,a>\},\quad f_3 = \{<1,a>,<2,b>,<3,b>\},$$
$$f_4 = \{<1,b>,<2,a>,<3,a>\},\quad f_5 = \{<1,b>,<2,a>,<3,b>\},$$
$$f_6 = \{<1,b>,<2,b>,<3,a>\},\quad f_7 = \{<1,b>,<2,b>,<3,b>\}。$$

这里的函数都是以序偶集合形式给出的，在可能的情况下，将其表示为解析形式更为直观。

5.1.3 特殊函数

[定义 5-4] 设有函数 $f: X \to Y$，若有 $y_0 \in Y$，使对所有的 $x \in X$，有 $f(x) = y_0$，称 f 是**常函数**。

[定义 5-5] 集合 X 上的恒等关系 I_X 称为 $X \to X$ 的**恒等函数**。

以下讨论 3 类特殊的函数，也体现了函数可能具有的特殊性质。

[定义 5-6] 若有函数 $f: X \to Y$，对于每个 $y \in Y$ 都可在 X 中找到原像，即 $f(X) = Y$，称 f 为**满射**（surejection），或**满映射**、**到上映射**、**映上**。符号描述为：

$$f \text{为满射} \Leftrightarrow \forall y(y \in Y \to \exists x(x \in X \wedge f(x) = y))。$$

[定义 5-7] 若有函数 $f: X \to Y$，在 X 中没有两个元素有相同的像，则称 f 是**单射**（injection），或**入射**、**一对一映射**。符号描述为：

$$f \text{为单射} \Leftrightarrow \forall x_1 \forall x_2((x_1 \in X \wedge x_2 \in X \wedge x_1 \neq x_2) \to f(x_1) \neq f(x_2))。$$

通常，可以用逆否命题来描述以方便证明时的叙述：

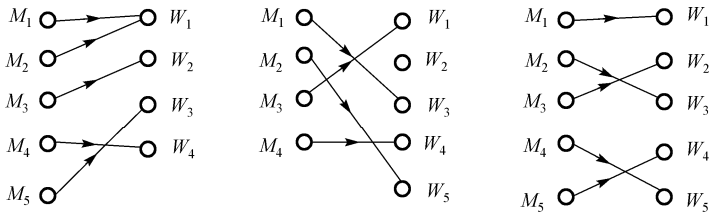
$$f \text{为单射} \Leftrightarrow \forall x_1 \forall x_2((x_1 \in X \wedge x_2 \in X \wedge f(x_1) = f(x_2)) \to x_1 = x_2)。$$

[辨析] 若 f 是 X 到 Y 的函数，函数 f 的单值性是要求一个 x 不能映射成 2 个 y，而单射函数要求的是 2 个 x 不能映射成一个 y。

[定义 5-8] 若函数 $f: X \to Y$ 既是满射又是单射，则称 f 为**双射**（bijection）或**一一对应**。

在 X 与 Y 是有限集时，集合间存在不同的函数能够说明集合元素个数的多少关系。例如，若将函数理解为在生活中对工人指派工作的关系，图 5-2 说明了集合间存在不同映射时的情况。

很明显，若存在 X 到 Y 的满射，为了使每个 y 都有不同的原像（函数的单值性要求），必须有足够多的原像 x，即 $|X| \geqslant |Y|$，它表示每个工作都要安排工人。若存在 X 到 Y 的单射，为了使每个 x 都有不同的像，必须有足够多的像 y，即 $|Y| \geqslant |X|$，它表示两个工人不能安排同一份工作。可见，若存在 X 到 Y 的双射，一定有 $|X| = |Y|$，它表示每个工人都安排唯一一份不同的工作。



(a) 满射　　(b) 单射　　(c) 双射

图 5-2

例 5-3　判断下述函数是否为单射、满射和双射？

(1) f：$\mathbf{R}\to\mathbf{R}$，$f(x)=x^2+2x-1$。

(2) f：$\mathbf{Z}^+\to\mathbf{R}$，$f(x)=\ln x$。

(3) f：$\mathbf{R}\to\mathbf{Z}$，$f(x)=\lfloor x\rfloor$，$\lfloor x\rfloor$为不大于 x 的最大整数。

(4) f：$\mathbf{R}\to\mathbf{R}$，$f(x)=2x+1$。

(5) f：$\mathbf{R}^+\to\mathbf{R}^+$，$f(x)=(x^2+1)/x$。

(6) f：$\mathbf{R}\to\mathbf{R}$，$f(x)=x^3$。

(7) f：$\mathbf{R}\times\mathbf{R}\to\mathbf{R}\times\mathbf{R}$，$f(<x,y>)=<x+y,x-y>$。

(8) f：$\mathbf{N}\to\mathbf{N}$，$f(x)=\begin{cases}0 & ,x\text{是奇数}\\ 1 & ,x\text{是偶数}\end{cases}$。

(9) f：$\mathbf{N}\to\{0,1\}$，$f(x)=\begin{cases}0 & ,x\text{是奇数}\\ 1 & ,x\text{是偶数}\end{cases}$。

(10) A 为集合，f：$A\to\mathscr{P}(A)$，$f(x)=\{x\}$。

(11) R 为集合 A 上的等价关系，f：$A\to A/R$，$f(a)=[a]_R$。

解　(1) 一般函数。开口向上的抛物线。

(2) 单射。因定义域仅为整数，部分实数无原像，故不是满射。

(3) 满射。对于 $n\in\mathbf{Z}$，区间$[n, n+1)$内的所有实数都是其原像。

(4) 双射。对于 $y\in\mathbf{R}$，$(y-1)/2$ 为其唯一原像。

(5) 一般函数，即 $y=f(x)=x+1/x$。因 x 和 $1/x$ 有相同的函数值，不是单射。当方程 $x^2-yx+1=0$ 无解时，y 没有原像，故不是满射。

(6) 双射。x 的原像为 $\sqrt[3]{x}$。

(7) 双射。对 $<u,v>\in\mathbf{R}\times\mathbf{R}$，$<(u+v)/2,(u-v)/2>$ 是其唯一的原像。

(8) 一般函数。除了 0、1 之外的整数都没有原像。

(9) 满射。

(10) 单射。$\mathscr{P}(A)$中的 $\varnothing$ 和不少于 2 个元素构成的子集都没有原像。

(11) 满射。每个 $[a]_R$ 都有原像 a。特别地，当每个 $|[a]_R|=1$，即 $R=I_A$ 时为双射。此映射称为**自然映射**。

[辨析] (8)和(9)只是值域有差别，可见集合本身对函数性质的影响很大。

对于一个函数是否具有某种性质的判断完全依赖其定义进行验证。

例 5-4 证明：若函数 f：$X \to Y$ 为单射，则 f 是 X 到 $f(X)$的双射。

证明 由于 f 为 $X \to Y$ 的单射，自然是 $X \to f(X)$ 的单射。对任意的 $y \in f(X)$，由 $f(X)$的定义，存在 $x \in X$，使 $y = f(x)$，故 f 是满射。结论成立。参见图 5-3。

例 5-5 证明：若函数 f：$X \to Y$ 是满射，则如下定义的关系 g：$Y \to \mathscr{P}(X)$是单射。

$$g(y) = \{x \mid x \in X \wedge f(x) = y\} \text{。}$$

证明 对于一般的函数 f，总会将若干 x 映射成一个 y，所有这些 x 构成了子集 $g(y)$，即 g 将每个 y 映射为它在 X 中的函数 f 下的原像集。图 5-3 说明了此函数中像与原像的对应关系。

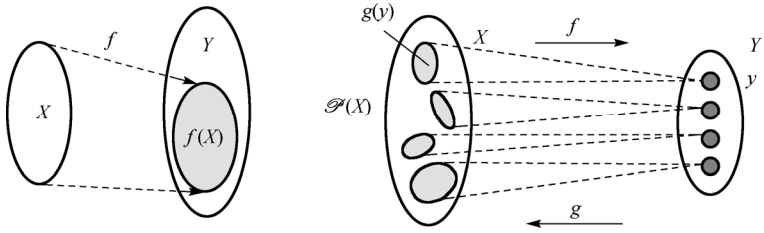


图 5-3

先说明 g 是函数。对 $\forall y \in Y$，按题意，$g(y)$为 y 的原像集，因 $g(y) \in \mathscr{P}(X)$，即 y 在 $\mathscr{P}(X)$中存在着像 $g(y)$，说明 g 的定义域为 Y。同时，因为 y 在函数 f 下的原像集只有一个，故 y 在关系 g 下只有一个像，满足单值性。故 g 是函数。

再说明 g 是单射。对于 $\forall y_1, y_2 \in Y$，假设 $g(y_1) = g(y_2) = S$。因 f 是满射，故 $S \neq \varnothing$。因此，存在 $x \in S \subseteq X$，使 $y_1 = f(x)$，$y_2 = f(x)$。因为 f 是函数，得 $y_1 = y_2$。因此，g 是单射。结论成立。

思考与练习 5.1

5-1 函数与普通关系有何差异？

5-2 什么样的函数是满射？什么样的函数是单射？什么样的函数是双射？

5-3 判断下述论断的正误：设有 X 到 Y 的关系 f，若 f 是函数，由单值性要求，对 $\forall x_1, x_2 \in X$，$x_1 \neq x_2$，必有 $f(x_1) \neq f(x_2)$。

5-4 设 A、B 为有限集合，$|A| = m$，$|B| = n$，m 和 n 应满足怎样的条件才能使下述结论为真？

(a) 存在 A 到 B 的单射。 (b) 存在 A 到 B 的满射。

(c) 存在 A 到 B 的双射。

5-5 设 $A = \{a, b, c\}$，$B = \{1, 2\}$，列出所有 A 到 B 的映射，并说明其中单射、满射和双射的个数。又，对于一般的有限集合 A 与 B，这些映射分别有多少个？

5-6 判断下列函数是否为单射、满射或双射。

(a) f：$\mathbf{I}\to\mathbf{I}$，$f(i)=i(\mathrm{mod}\ 3)$。　　(b) f：$\mathbf{I}\to\mathbf{N}$，$f(i)=|2i|+1$。

(c) f：$\mathbf{N}\to\mathbf{N}$，$f(n)=n^2+1$。　　(d) f：$\mathbf{Z}\to\mathbf{Z}$，$f(x)=3x-11$。

(e) f：$\mathbf{R}\to\mathbf{R}$，$f(x)=5x+8$。　　(f) f：$\mathbf{N}^2\to\mathbf{N}$，$f(<m,n>)=m^n$。

(g) f：$\mathbf{N}\to\mathbf{N}^2$，$f(x)=<x,x+1>$。　　(h) f：$\mathbf{N}^2\to\mathbf{N}$，$f(<m,n>)=m+n$。

(i) f：$\mathbf{R}\to\mathbf{R}^+$，$f(x)=\mathrm{e}^x$。　　(j) f：$\mathbf{R}^2\to\mathbf{C}$，$f(<x,y>)=x+\mathrm{i}y$。

(k) f：$(\mathscr{P}(A))^2\to(\mathscr{P}(A))^2$，$f(<X,Y>)=<X\cup Y,X\cap Y>$。

5-7　设 f 和 g 是函数，证明 $f\cap g$ 也是函数（注意定义域可能与 f 和 g 不同）。

5-8　构造由区间(2,5)到(13,7)之间的单射（非满射）和双射。

5.2　函数的逆与复合

5.2.1　双射的反函数

作为一般关系，可以对函数 f：$X\to Y$ 求逆：

$$f^{-1}=\{<y,x>|<x,y>\in f\}。$$

不过，一个普通函数的逆可能不再是函数，这是因为若 f 不是满射，则逆关系 f^{-1} 的定义域不能充满 Y。若 f 不是单射，其逆 f^{-1} 不满足函数的单值性要求。可见，只有双射函数的逆才是函数。

[定理 5-1] 若 f 是 X 到 Y 的双射函数，则 f^{-1} 是 Y 到 X 的双射函数。

证明　先说明 f^{-1} 是函数。

对 $\forall y\in Y$，因 f 是满射，有 $x\in X$，使 $<x,y>\in f$，即 $<y,x>\in f^{-1}$，说明 $\mathrm{dom}\ f^{-1}=Y$。

若 $f^{-1}(y)=x_1$，且 $f^{-1}(y)=x_2$，必有 $x_1=x_2$。否则，有 $f(x_1)=y$，$f(x_2)=y$，与 f 是单射矛盾，故 f^{-1} 是单值的。因此，f^{-1} 是函数。

再说明 f^{-1} 是满射。对 $\forall x\in X$，因 f 是函数，有 $y\in Y$，使 $<x,y>\in f$，即 $<y,x>\in f^{-1}$。

再说明 f^{-1} 是单射。若 $f^{-1}(y_1)=f^{-1}(y_2)=x$，则 $f(x)=y_1$ 且 $f(x)=y_2$，由 f 的单值性知，$y_1=y_2$。因此，f^{-1} 是双射。结论成立。

通常，双射函数 f 的逆 f^{-1} 被称为**反函数**（invertible function）。

5.2.2　函数的复合

[定义 5-9] 设函数 f：$X\to Y$，g：$Y\to Z$，则 f 与 g 的**复合**（composition）或**合成**为

$$g\circ f=\{<x,z>|x\in X\wedge z\in Z\wedge\exists y(y\in Y\wedge y=f(x)\wedge z=g(y))\}$$

[辨析] 函数的复合与一般关系复合的内涵一致，但 g 和 f 的书写顺序相反，也称为 g 对 f 的左复合。普通关系 R 和 S 的复合记作 $R\circ S$，但函数 f 与 g 的复合记作 $g\circ f$，其目的是为了满足 $g\circ f(x)=g(f(x))$ 的要求。

应注意，一些书中将f与g的复合记作$f\circ g$，此时有$f\circ g(x)=g(f(x))$。但本书中提到的函数f与g的复合函数总是指g对f的左复合函数。

[辨析] 本质上，若函数f：$A\to B$，g：$C\to D$，且$f(A)\subseteq C$，即f的像集为C的子集，则可进行函数的复合。

[定理 5-2] 两个函数f和g的复合$g\circ f$是一个函数。

证明 对$\forall x\in X$，因f是函数，有$y\in Y$，使$f(x)=y$。又因为g是函数，有$z\in Z$，使$g(y)=z$。于是，有

$$g\circ f(x)=g(f(x))=g(y)=z\text{。}$$

即$g\circ f$的定义域为X。

若$g\circ f(x)=z_1$且$g\circ f(x)=z_2$，即

$$g(f(x))=z_1,\quad g(f(x))=z_2\text{。}$$

因为g的单值性，有$z_1=z_2$。所以，$g\circ f$是函数。

例 5-6 求下述函数的复合函数。

(1) $A=\{1,2,3\}$，$B=\{p,q\}$，$C=\{r,s\}$，f：$A\to B$且有

$$f=\{<1,p>,<2,p>,<3,q>\},$$

g：$B\to C$且有

$$g=\{<p,s>,<q,s>\}\text{。}$$

求$g\circ f$。

(2) $f,g,h\in\mathbf{R}^{\mathbf{R}}$，且有

$$f(x)=x+3,\quad g(x)=2x+1,\quad h(x)=x/2\text{。}$$

求$f\circ g\circ h$。

(3) $f,g\in\mathbf{R}^{\mathbf{R}}$，且有

$$f(x)=\begin{cases}x^2 & ,x\geqslant 3\\ -2 & ,x<3\end{cases},\quad g(x)=x+2\text{。}$$

求$f\circ g$和$g\circ f$。

解 (1) $g\circ f=\{<1,s>,<2,s>,<3,s>\}$。

(2) $f\circ g\circ h(x)=f(g(h(x)))=g(h(x))+3=2h(x)+4=x+4$。

(3) $f\circ g(x)=f(g(x))=\begin{cases}g(x)^2 & ,g(x)\geqslant 3\\ -2 & ,g(x)<3\end{cases}=\begin{cases}(x+2)^2 & ,x\geqslant 1\\ -2 & ,x<1\end{cases}$。

$$g\circ f(x)=g(f(x))=f(x)+2=\begin{cases}x^2+2 & ,x\geqslant 3\\ 0 & ,x<3\end{cases}\text{。}$$

[定理 5-3] 函数复合运算满足结合律，即$(f\circ g)\circ h=f\circ(g\circ h)$。

证明 略。

[定理 5-4] 设 $g\circ f$ 是一个复合函数，则

(1) 若 f 和 g 是满射，则 $g\circ f$ 是满射。

(2) 若 f 和 g 是单射，则 $g\circ f$ 是单射。

(3) 若 f 和 g 是双射，则 $g\circ f$ 是双射。

证明　设函数 f：$X\to Y$，g：$Y\to Z$。

(1) 对 $\forall z\in Z$，因为 g 是满射，有 $y\in Y$，使 $g(y)=z$。又因为 f 是满射，有 $x\in X$，$f(x)=y$。于是，$g\circ f(x)=z$，故 $g\circ f$ 是满射。

(2) 若 $g\circ f(x_1)=g\circ f(x_2)$，则 $g(f(x_1))=g(f(x_2))$。因为 g 是单射，有 $f(x_1)=f(x_2)$。又因为 f 是单射，有 $x_1=x_2$，故 $g\circ f$ 是单射。

由(1)、(2)知(3)成立。

5.2.3　函数运算的性质

[定理 5-5] 设函数 f：$X\to Y$，则 $f=f\circ I_X=I_Y\circ f$。

证明　仅证明 $f=f\circ I_X$。

显然，f 与 $f\circ I_X$ 的定义域和值域都相同，且对 $\forall x\in X$，有

$$f\circ I_X(x)=f(I_X(x))=f(x)。$$

故 $f=f\circ I_X$，结论成立。

[定理 5-6] 设函数 f：$X\to Y$ 有反函数 f^{-1}，则 $f^{-1}\circ f=I_X$，$f\circ f^{-1}=I_Y$。

证明　仅证明 $f^{-1}\circ f=I_X$。

显然，$f^{-1}\circ f$ 与 I_X 的定义域和值域都相同，且对 $\forall x\in X$，若 $y=f(x)$，有

$$f^{-1}\circ f(x)=f^{-1}(f(x))=f^{-1}(y)=x=I_X(x)。$$

故 $f^{-1}\circ f=I_X$，结论成立。

[定理 5-7] 若 f：$X\to Y$ 是双射，则 $(f^{-1})^{-1}=f$。

证明　显然，$(f^{-1})^{-1}$ 与 f 的定义域和值域都相同。对 $\forall x\in X$，若 $y=f(x)$，有

$$f^{-1}(y)=x,$$

$$(f^{-1})^{-1}(x)=y=f(x)。$$

故 $(f^{-1})^{-1}=f$，结论成立。

[定理 5-8] 若函数 f：$X\to Y$，g：$Y\to Z$ 都是双射，则 $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$。

证明　首先，$(g\circ f)^{-1}$ 与 $f^{-1}\circ g^{-1}$ 有相同的定义域和值域。

其次，对 $\forall z\in Z$，因为 g 为双射，有 $y\in Y$，使 $z=g(y)$。同样，因 f 为双射，有 $x\in X$，使 $y=f(x)$。因此，$g\circ f(x)=z$，即 $(g\circ f)^{-1}(z)=x$。

因为 $f^{-1}(y)=x$，$g^{-1}(z)=y$，有 $f^{-1}\circ g^{-1}(z)=f^{-1}(g^{-1}(z))=f^{-1}(y)=x$。于是，有

$$(g\circ f)^{-1}(z)=f^{-1}\circ g^{-1}(z)\text{。}$$

故 $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$，结论成立。

[辨析] 应该说，函数相等的证明都是从定义出发，说明三要素（定义域、值域和对应关系）相同，但也可以直接证明集合相等。如考虑 $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$ 的证明。

对 $\forall <z,x>$，有

$\forall <z,x>\in (g\circ f)^{-1}$

$\Rightarrow <x,z>\in g\circ f \Rightarrow \exists y(<x,y>\in f\wedge <y,z>\in g)$

$\Rightarrow \exists y(<z,y>\in g^{-1}\wedge <y,x>\in f^{-1})\Rightarrow <z,x>\in f^{-1}\circ g^{-1}$。

故 $(g\circ f)^{-1}\subseteq f^{-1}\circ g^{-1}$。同理可证 $f^{-1}\circ g^{-1}\subseteq (g\circ f)^{-1}$。

[辨析] 由于函数采用左复合，在采用序偶集合进行分析论证时，必须注意函数复合与普通关系复合的差异。对于定义在 X 到 Y 和 Y 到 Z 的关系 f 和 g，且 $<x,y>\in f$，$<y,z>\in g$，则有结论 $<x,z>\in f\circ g$。若 f 和 g 为函数，其结论为 $<x,z>\in g\circ f$。

思考与练习 5.2

5-9 什么样的函数存在逆函数？

5-10 函数复合与普通关系复合在表示上有何差别？复合函数采用新的表示法有什么好处？

5-11 计算 2 个函数的复合。

(a) σ：$\mathbf{R}\to\mathbf{R}$，$\sigma(x)=x^2+2x+1$，τ：$\mathbf{R}\to\mathbf{R}$，$\tau(x)=x/2$，求 $\sigma\circ\tau$ 和 $\tau\circ\sigma$。

(b) 设 f，$g\in\mathbf{N}^{\mathbf{N}}$，有

$$f(x)=\begin{cases}x+1 & ,x=0,1,2,3\\ 0 & ,x=4\\ x & ,x\geqslant 5\end{cases}\text{，}\quad g(x)=\begin{cases}x/2 & ,x\text{为偶数}\\ 3 & ,x\text{为奇数}\end{cases}\text{。}$$

求 $g\circ f$，并判断其是否为单射或满射。

5-12 设函数 f：$X\to Y$，证明 $f=I_Y\circ f$。

5-13 设 A 为非空集合，举例说明存在 f：$A\to A$，且 $f\neq I_A$，使 $f\circ f=I_A$。存在这样的双射吗？

5-14 设有 f：$A\to B$，g：$B\to A$，满足 $g\circ f=I_A$，$f\circ g=I_B$，证明 f 是双射且 $f^{-1}=g$。

5-15 验证函数复合运算满足结合律。

5-16 设有 f：$A\to B$，g：$B\to C$，证明：

(a) 若 $g\circ f$ 为满射，则 g 是满射。　　(b) 若 $g\circ f$ 为单射，则 f 是单射。

5.3 集合的基数

一个集合中含有的元素多少应如何度量？对于有限集合，可以统计其元素的个数，但无限集

的元素无法用“多少个”来表达。否则，就会产生无法解释的现象。

例如，一家旅店有无穷多单人客房，且已客满。当新来一位客人时，店主欣然接纳，且只是将一号房的客人移到二号房，二号房的客人移到三号房，等等。最后，让新客人住进腾出的一号房。如果最初的客人集合记作 $\mathbf{Z}^+=\{1,2,3,\cdots\}$，增加新客人后的集合记作 $\mathbf{N}=\{0,1,2,3,\cdots\}$，而客房个数并无改变，等同于说 $\mathbf{Z}^+$与 $\mathbf{N}$ 有相同多个元素，但后者明显比前者多了元素 0。这就是著名的伽利略悖论，它说明需要对集合元素的“个数”进行重新度量。

一个集合 A 中含有元素多少的度量称为集合的**基数**（cardinality）或**势**，记作 $|A|$（或 $\operatorname{card}A$，或 $K[A]$，或 $\overline{\overline{A}}$）。基数是元素个数的推广，对于有限集，基数就是其元素个数。集合的基数或势越大，含有的元素越多。

5.3.1　集合等势

对函数和有限集合的讨论告诉我们，可以通过集合之间的映射来衡量元素个数的多少。两个相同大小的有限集合之间一定存在双射，即元素之间的一一对应，反之亦然。这种结果可以用于对任意集合间的元素多少是否一致的衡量。

[定义 5-10] 若集合 A 和 B 之间存在双射，则称 A 与 B **等势**（或**基数相同**、**对等**），记作 $|A|=|B|$，或 $\operatorname{card}A=\operatorname{card}B$。在将等势作为一种关系运算看待时记作 $A\sim B$。

例如，$A=\{1,2,3\}$，$B=\{a,b,c\}$，构造双射 f：$A\to B$，满足：

$$f(1)=a,\ f(2)=b,\ f(3)=c\ 。$$

这就证明了 $|A|=|B|$。

例 5-7　证明自然数集 $\mathbf{N}$ 与非负偶数集 M 等势。

证明　构造函数 f：$\mathbf{N}\to M$，满足：

$$f(n)=2n,n\in\mathbf{N}。$$

因为 f 是双射，有 $|\mathbf{N}|=|M|$。

[辨析] 从感觉上，偶数只有自然数的“一半多”，但二者的基数是相同的，这也说明用“个数”来表述无限集合元素的多少是不对的。

构造 2 个集合间的双射需要掌握一些技巧。例如，两个区间内的实数集之间的双射可以利用线性函数得到，$(-\infty,+\infty)$ 与 $(-\infty,+\infty)$、$(-\infty,0)$、$(0,+\infty)$ 之间的双射可使用 $\ln x$、e^x 等函数构造，有限区间与无穷区间的双射可用 $\tan x$ 或其反函数 $\arctan x$ 构造。一般可以采用待定系数法。

例 5-8　证明 $\mathbf{R}\sim(0,1)$。

证明　设 f：$\mathbf{R}\to(0,1)$，$f(x)=a\cdot\arctan(x)+b$。将 $-\infty$ 与 0 对应，$+\infty$ 与 1 对应，有

$$\begin{cases}f(-\infty)=a\cdot\arctan(-\infty)+b=a(-\pi/2)+b=0\\ f(+\infty)=a\cdot\arctan(+\infty)+b=a(+\pi/2)+b=1\end{cases}。$$

解方程得到系数 $a=1/\pi$，$b=1/2$。

因为 $f(x)=\arctan(x)/\pi+1/2$ 是双射，结论成立。

5.3.2 有限集与无限集

[定义 5-11] 设 A 是集合，如果存在一个子集 $B \subseteq A$ 与自然数集 **N** 等势，则称 A 是**无限集**（infinite set），否则称 A 为**有限集**（finite set）。

当然，自然数集本身是无限集。因为非负偶数集与 **N** 等势，故非负偶数集也是无限集。

例 5-9 证明(0,1)是无限集。

证明 记 $A=\{1/2,1/3,\cdots,1/n,\cdots\}$，有 $A \subseteq (0,1)$。构造 f：$A \to \mathbf{N}$：

$$f(1/i)=i-2, i=2,3,\cdots。$$

因为 f 是双射，说明 A～**N**，故结论成立。

[延伸] 定义 5-11 通过先定义无限集而后得到有限集，也可以先定义有限集，再得到无限集：对于集合 A，如果存在自然数 n，使集合$\{0, 1, 2, \cdots, n-1\}$～A，则 A 为有限集。否则 A 为无限集。

5.3.3 可数集与不可数集

无限集的基数并非都是相同的。

[定义 5-12] 与自然数集 **N** 等势的集合称为**可数集**（countable set）或**可列集**。不可数的无限集称为**不可数集**(uncountable set)。

[理解] “可数”就是指定集合中的某个元素，总可以从头数到它。例如，对于 **N**，无论指定一个多大的整数 n，总可以从 0 逐个遍历所有整数，直到 n 结束。如果存在集合 A 到 **N** 的双射，就可以将 A 的元素与 **N** 对应地排列，从而 A 也是可数的。

为什么可数集又称为可列集？若 A 是可数集，则存在双射 f：$\mathbf{N} \to A$，于是，A 的元素可列成 $a_0=f(0), a_1=f(1), a_2=f(2), \cdots$ 的形式。

可见，A 是可数集等同于 A 的元素可按自然数的顺序排列。

通常，所有有限集和与自然数集 **N** 基数相同的集合都是可数的，合称为**至多可数集**（在不至于混淆时，也可以将有限集与可数无限集统称为可数集）。同时，无限集被分为两类，一类是可数（无限）集，另一类是不可数（无限）集。

可数集是一个大的“家族”，容易证明，可数子集的无限子集、两个可数集的交或并甚至可数个可数集的并都是可数集。

[定理 5-9] 可数集的无限子集是可数集。

证明 设 A 是可数集，B 为 A 的无限子集。若 A 的元素可排列成如下形式：

$$a_0, a_1, \cdots, a_n, \cdots。$$

对于 B 的任意元素，从 a_0 开始，沿此排列顺序搜索并不断舍弃非 B 的元素，即可数到 B 的指定元素，并建立起 B 与 **N** 之间的一一对应：

$$a_{i_0}, a_{i_1}, \cdots, a_{i_n}, \cdots。$$

故 B 是可数集。

例 5-10　证明可数个可数集的并是可数集。

证明　记 $A_i=\{a_{i1},a_{i2},a_{i3},\cdots\}$，$i=1,2,3,\cdots$ 是可数个可数集，且它们互不相交。令 $A=\bigcup_{i=1}^{+\infty}A_i$，对其元素作如图 5-4 的排列。

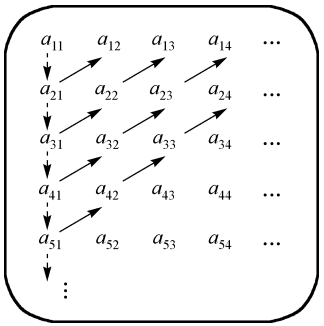


图 5-4

图中排列方式的规律是每条斜线上的元素的两个下标之和相同。从 a_{11} 开始，按箭头方向所指的下标之和逐渐增大的方式排列，有

$$a_{11},\ a_{21},\ a_{12},\ a_{31},\ a_{22},\ a_{13},\ a_{41},\ a_{32},\ a_{23},\ a_{14},\ a_{51},\ a_{42},\ a_{33},\ a_{24},\ a_{15},\cdots$$

这就建立起了 A 与 **N** 之间的一一对应，故 A 是可数集。

如果上述集合是有限个，或者其中包括有限集，或者集合之间相交，那么，A 或者是有限集，或者是图 5-4 所列可数集的一个无限子集，故也是可数集。因此，可以将此论断叙述为：至多可数个至多可数集的并是至多可数集。

图 5-4 中采用的元素排列及证明方法称为**康托尔对角线论证法**。

例 5-11　证明整数集 **Z**、**N**×**N** 和有理数集 **Q** 是可数集。

证明　构造函数 f：$\mathbf{Z}\to\mathbf{N}$，满足

$$f(n)=\begin{cases}2n & ,n\geqslant 0\\ -2n-1 & ,n<0\end{cases}。$$

显然 f 是双射，故 **Z** 是可数的。

N×**N** 集合仍可以根据康托尔对角线论证法来排列元素，如图 5-5 所示。因此是可数的。

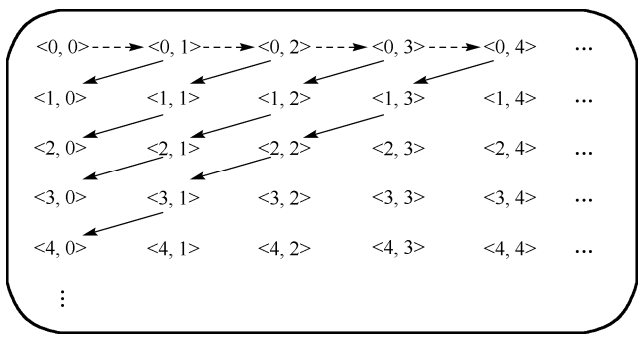


图 5-5

[延伸] 事实上，根据图 5-5 中的排列顺序也可以实际构造出 **N**×**N** 与 **N** 之间的双射[3]：

$$f(m,n)=\frac{1}{2}(m+n)(m+n+1)+m。$$

有理数集 **Q** 可以分为正有理数集 $\mathbf{Q}^+$、负有理数集 $\mathbf{Q}^-$ 和 0，即

$$\mathbf{Q}=\mathbf{Q}^+\cup\mathbf{Q}^-\cup\{0\}。$$

因为任何有理数可表示成 p/q（p、q 为整数），写成<p,q>的形式可知，$\mathbf{Q}^+$ 只是 $\mathbf{N}\times\mathbf{N}$ 的一个无限子集，因此是可数的，进而 $\mathbf{Q}^+\cup\mathbf{Q}^-\cup\{0\}$ 也是可数的。

[辨析] 对角线论证法可以有各种排列方式，如图 5-4 与图 5-5 所示，但核心是以有限的方式轮流访问到每个集合的元素。

为了方便比较，一般将可数集的基数（即自然数 **N** 的基数）记作 $\aleph_0$，读作“阿列夫零”。那么，是否有不可数的集合呢？

[定理 5-10] 实数集 **R** 是不可数的。

首先证明(0,1)区间内的实数是不可数的。否则，所有这些纯小数可以排列成如下形式：

$$a_1 = 0.\boldsymbol{a}_{11}a_{12}a_{13}a_{14}a_{15}\cdots$$
$$a_2 = 0.a_{21}\boldsymbol{a}_{22}a_{23}a_{24}a_{25}\cdots$$
$$a_3 = 0.a_{31}a_{32}\boldsymbol{a}_{33}a_{34}a_{35}\cdots$$
$$a_4 = 0.a_{41}a_{42}a_{43}\boldsymbol{a}_{44}a_{45}\cdots$$

其中的每个 a_{ij} 都是 0～9 中的数字。现构造一个小数 $b=0.b_1b_2b_3b_4\ldots$，使 $b_i\neq a_{ii}$，即 b 与数列中第 i 个数的第 i 位是不同的。那么，上述数列中一定不包含 b，这与所有数可列矛盾。因此，(0,1)区间内的实数是不可数的。

因为(0,1)区间内的实数与实数集 **R** 具有相同的基数，因此，**R** 是不可数的。

实数集 **R** 的基数记作 $\aleph$，读作“阿列夫”。还可以将此基数记作 C，并称其为“连续统的势”，因为具有基数 C 的集合被称为“连续统”（continuum）。

5.3.4 基数比较

为了说明两个集合具有相同的基数需要构造双射，这通常是困难的，可以采用只构造单射的方法进行简化。

[定义 5-13] 若存在集合 A 到 B 的单射，则称为 A 的**基数不大于** B 的基数，即 $|A|\leqslant|B|$。若仅存在集合 A 到 B 的单射而不存在双射，则称为 A 的**基数小于** B 的基数，即 $|A|\lhd|B|$。

[定理 5-11] 对任意集合 A 和 B，若 $|A|\leqslant|B|$ 且 $|B|\leqslant|A|$，则 $|A|=|B|$。

此定理称为 **Cantor-Schroder-Bernstein 定理**，证明略。它说明可以通过构造两个单射 f：$A\to B$ 和 g：$B\to A$ 来证明集合 A 与 B 具有相同的基数。

例 5-12 证明[0,1]与(0,1)有相同的基数。

证明 分别构造单射 f：$(0,1)\to[0,1]$ 和 g：$[0,1]\to(0,1)$，满足

$$f(x)=x,\ \ g(x)=\frac{x}{2}+\frac{1}{4}。$$

结论成立。

例 5-13 证明 $|\mathbf{N}\times(0,1)|=\aleph$。

证明 考虑到集合 $\mathbf{R}^+$ 和(0,1)的基数都是 $\aleph$。首先构造单射 f：$\mathbf{N}\times(0,1)\to\mathbf{R}^+$，满足

$$f(<n,x>)=n+x,\ \ n\in\mathbf{N}。$$

因此，有$|\mathbf{N}\times(0,1)|\leqslant\aleph$。

再构造单射 g：$(0,1)\to\mathbf{N}\times(0,1)$，满足

$$g(x)=<0,x>。$$

于是，有$\aleph\leqslant|\mathbf{N}\times(0,1)|$。结论成立。

[定理 5-12] 若 A 是有限集，则$|A|<\aleph_0<\aleph$；若 A 是无限集，则$\aleph_0\leqslant|A|$。

证明　略。

[定理 5-13] 若 A 是一个集合，则$|A|<|\mathscr{P}(A)|$。此定理称为 **Cantor 定理**。

此定理说明，任何集合的幂集的基数总是大于原集合的基数。因此，不存在最大的集合和最大的基数。

[延伸] 集合的基数和序数是有关集合元素的两个基本词汇，前者表示集合中含有元素多少，而后者用来刻画一个元素在集合中的位置。

集合基数的典型应用之一体现在有限计数问题上。对于无限集，证明两集合的基数相同是最基本的问题，并存在一些典型的方法。另外，对无限集合基数的研究还涉及一些尚未得到解决的问题，如“连续统假设”等[3, 30, 31]。

思考与练习 5.3

5-17　证明 $\mathbf{N}\times\mathbf{N}$ 是无限集。

5-18　利用构造双射的方法证明集合 A 与 B 基数相同。

(a) $A=(5,9)$，$B=(7,17)$。　　(b) $A=\mathbf{R}$，$B=(0,+\infty)$。

(c) $A=[0,1)$，$B=(1/4,1/2]$。　　(d) $A=\mathbf{Z}-\{-1,0,1\}$，$B=\mathbf{N}-\{0,1\}$。

(e) $A=\{1/(2n)\mid n\in\mathbf{Z}^+\}\cup\{1/(2n+1)^2\mid n\in\mathbf{N}\}$，$B=\mathbf{N}$。

5-19　设 $A\sim B$，$C\sim D$，构造双射证明 $A\times C\sim B\times D$。

5-20　设集合$\mathcal{A}$为由集合构成的集合，证明$\mathcal{A}$上的等势关系是等价关系。

5-21　构造双射证明两个可数集的并是可数集。

5-22　证明任意无限集必与其某个真子集等势。

5-23　无理数集是可数集吗？证明你的结论。

5-24　证明(0,1)与(0,1]等势。

5-25　集合$\{<m,n>\mid m,n\in\mathbf{Q}\}$、$(0,1)-\{1/n\mid n\in\mathbf{Z}^+\}$的基数各是多少？

5-26　回答下述问题。

(a) 无限集都是可数的吗？

(b) 存在基数最大的集合吗？如何得到一个比集合 A 的基数更大的集合？

(c) 在一个集合 A 中增加一个新的元素得到集合 B，$|A|<|B|$ 成立吗？增加多少元素会使集合的基数发生变化？

第 6 章　运算与代数系统

运算是指对集合元素的加工、处理和变换，集合与其上定义的运算构成了各种代数系统，也称为代数结构，它们是近世代数（也称为抽象代数）研究的中心内容，在现代数学、计算机科学和编码理论等领域具有很多重要的应用。

6.1　运算及其性质

6.1.1　*n* 元运算

在一个集合上构造映射之后，可以利用映射得到集合元素的像，从而形成了运算。

[定义 6-1] 设 A 是一个非空集合，一个映射 f：$A^n \to A$ 称为 A 上的 ***n* 元代数运算**，简称 ***n* 元运算**（*n*-ary operation）。其中，$n \geqslant 1$ 为自然数，称为运算的**元**、**阶**或**目**。

最常见的运算为一元运算和二元运算，如程序设计语言中广泛使用的取正、取负、否定和按位取反为一元运算，算术运算、关系运算、其他逻辑运算、按位运算等都是二元运算。

例如，f：$\mathbf{N}^2 \to \mathbf{N}$，$f(<x,y>)=x+y$ 是自然数集 $\mathbf{N}$ 上定义的二元运算，代表普通加法。

又如，设 f：$\mathbf{Z} \to \mathbf{Z}$，$f(x)=|x|$，则 f 是 $\mathbf{Z}$ 上的一元运算，即取绝对值运算。

通常，常见运算多用 * 、∘、⊙、☆等运算符表示，较少用 f、g 等字符描述，这样可以把 $f(<x,y>)=z$ 简记为 $x \circ y = z$ 的形式。

[辨析] 运算定义中的“$\to A$”是重要的要求，它要求运算对原集合“封闭”，即运算后的结果必须属于原集合。例如，除法“/”不是 $\mathbf{R}$ 上的二元运算，因为除数为 0 时无意义，即运算不封闭。减法“–”不是 $\mathbf{R}^+$ 上的二元运算，因为对于两个正整数 x、y，若 $x<y$，其差 $x-y$ 为负数，不属于 $\mathbf{R}^+$。

原则上，可以将一个映射 f：$A^n \to B$ 作为 n 元运算的定义，但这种情况下，总需要考虑运算结果对 A 的封闭性，即应该有 $B \subseteq A$，否则没有什么实际意义。

例 6-1　设 $A=\{x \mid x=2^n, n \in \mathbf{N}\}$，问乘法和加法是否为 A 上的二元运算？

解　问题等同于衡量运算是否对 A 封闭。对 A 的任意两个元素 $x=2^p$ 和 $y=2^q$，因为

$$x \times y = 2^{p+q} \in A \text{。}$$

但 $p=1$ 且 $q=2$ 时，有

$$2^1 + 2^2 = 6 \notin A \text{。}$$

故乘法 × 是 A 上的二元运算，加法+不是 A 上的二元运算。

实数集 **R** 上的 + 、 − 和 × ，集合 A 的幂集 $\mathscr{P}(A)$上的 ∪、∩、 − 和 ⊕，一个集合 A 到 A 的函数集 A^A 上的函数复合运算 ∘，n 阶（$n \geqslant 1$）实数矩阵集合上的矩阵加法和乘法都是二元运算。C 语言中实数集 **R** 上的“？：”是一个三元运算。

有限集合上的运算可用运算表来描述。例如，集合 $A=\{1,2,3,4\}$，运算 * 定义为 $x*y=\max(x,y)$，则运算可由表 6-1 来表示。

表 6-1

*	1	2	3	4
1	1	2	3	4
2	2	2	3	4
3	3	3	3	4
4	4	4	4	4

第 i 行首元素*第 j 列首元素

6.1.2　二元运算的主要性质

这里主要讨论二元运算的一些共性。以下设 * 和 ∘ 是集合 A 上的二元运算。

[定义 6-2] 若对 $\forall x,y \in A$，有

$$x*y = y*x。$$

则称 * 是**可交换**的，或称 * 满足**交换律**(commutative)。

例如，实数集上的加法和乘法是可交换的，但减法不是可交换的。

例 6-2　定义有理数集 **Q** 上的 * 运算为：对 $\forall a,b \in \mathbf{Q}$，有 $a*b=a+b-a\cdot b$，其中的+和 · 为普通加法和乘法运算，则 * 是可交换的。

证明　对 $\forall a,b \in \mathbf{Q}$，有

$$a*b=a+b-a\cdot b=b+a-b\cdot a=b*a\ 。$$

故交换律成立。

[定义 6-3] 若对 $\forall x,y,z \in A$，有

$$x*(y*z)=(x*y)*z。$$

则称 * 运算是**可结合**的，或称 * 运算满足**结合律**(associative)。

例如，实数集上的加法和乘法是可结合的，但减法不是可结合的，如$(7-3)-2 \neq 7-(3-2)$。

例 6-3　设 A 为非空集合，运算 * 定义为：对 $\forall a,b \in A$，有 $a*b=b$，则 * 是可结合的。

证明　$\forall a,b,c \in A$，有

$$a*(b*c)=b*c=c=(a*b)*c\ 。$$

故结合律成立。

如果一个运算 * 满足结合律，那么，只由该运算符组成的表达式中强调“优先次序”的括号可以去掉，否则不可以。例如，实数集上的加法满足结合律，$a+(b+c)=a+b+c$，但减法不满足结合律，即 $a-(b-c) \neq a-b-c$，必须用括号强调优先次序。

如果一个运算*满足结合律，且每次参加运算的是同一个元素，可以用该元素的幂来表示，即

$$a^n = \underbrace{a*a*\cdots*a}_{n个}。$$

称其为 a 的 ***n* 次幂**，其中 n 为 a 的**指数**。

容易验证如下算律：

$$a^n * a^m = a^{n+m}, (a^n)^m = a^{nm},\ n,m \in \mathbf{Z}^+。$$

[辨析] 对于加法，2^m 意为 m 个 2 相加，$2^3+2^4=6+8=2^7$；对于乘法，2^m 意为 m 个 2 相乘，$2^3\times 2^4=128=2^7$。这里的幂含义不同，不要将 a^n 误认为总是 n 个 a 相乘。

[定义 6-4] 如果有 $x\in A$，使 $x^2=x*x=x$，称 x 是*运算的**等幂元**（或**幂等元**）。若对 $\forall x\in A$，有

$$x^2 = x。$$

则称*是**等幂**（或**幂等**）的，或称*满足**等幂律**(或**幂等律**，idempotent)。

例如，幂集上的$\cup$、$\cap$运算都是等幂运算。例 6-3 中的*运算也是等幂运算。

[定义 6-5] 若对 $\forall x,y,z\in A$，有

$$x*(y\circ z)=(x*y)\circ(x*z),$$

$$(y\circ z)*x=(y*x)\circ(z*x)。$$

则称*对∘是**可分配**的，或称*对∘满足**分配律**（distributive）。

例如，实数集上的乘法对加法、n 阶多项式和矩阵上的乘法对加法都是可分配的，幂集上的$\cup$和$\cap$是互相可分配的。

[辨析]（可）分配律不是对称的，即*对∘可分配不能保证∘对*也可分配。例如，实数乘法×对加法+可分配，反之不可分配。

[定义 6-6] 设*和∘是可交换的二元运算，若对 $\forall x,y\in A$，有

$$x*(x\circ y)=x,$$

$$x\circ(x*y)=x。$$

则称运算*和运算∘满足**吸收律**（absorptive）。

例如，幂集上的$\cup$和$\cap$满足吸收律。又如，定义自然数集 $\mathbf{N}$ 上的运算*和∘，使对 $\forall x,y\in\mathbf{N}$，有

$$x*y=\max(x,y),\ x\circ y=\min(x,y)。$$

则二者满足吸收律。

[辨析] 吸收律是相互的，且要求运算本身是可交换的。

运算的各种性质都是通过逐个验证元素的运算结果来说明的。

思考与练习 6.1

6-1　设集合 $A=\{1,2,3,\cdots,10\}$，说明下述函数是否为 A 上的二元运算，其中的 GCD、LCM 分别是最大公约数和最小公倍数。

(a) $\max(x,y)$。　(b) $\min(x,y)$。

(c) $\mathrm{GCD}(x,y)$。　(d) $\mathrm{LCM}(x,y)$。

(e) $f(x)=$ 满足 $x\leqslant m\leqslant y$ 的质数 m 的个数。

6-2　集合 $A=\{a,b,c\}$上可定义多少个二元运算？

6-3　设集合 $A=\{1,2,3\}$，定义 A 上的*运算和 Δ 运算如表 6-2 和表 6-3 所示，分析运算的幂等性和可交换性。

表 6-2

*	1	2	3
1	1	2	3
2	2	2	3
3	3	3	2

表 6-3

Δ	1	2	3
1	1	2	3
2	2	2	2
3	3	1	3

6-4　对于 **R** 上的 6 种二元运算加法、减法、乘法、max、min 和$|x-y|$，分别说明其是否满足可结合性和可交换性。

6-5　设 m 是任意正整数，$N_m=\{0,1,2,\cdots,m-1\}$，在 N_m 上定义模 m 加法运算 $+_m$ 和模 m 乘法运算 $\times_m$ 如下：

$$i+_m j=(i+j)(\mathrm{mod}\ m),$$

$$i\times_m j=(i\cdot j)(\mathrm{mod}\ m)。$$

(a) 写出<N_6，$+_6$>和<N_6，$\times_6$>的运算表；

(b) 证明 $\times_m$ 对 $+_m$ 是可分配的。

6-6　定义 $\mathbf{Z}^+$上的两个运算为：对 $\forall a,b\in\mathbf{Z}^+$，有

$$a*b=a^b,\quad a\Delta b=a\cdot b。$$

其中的 $\cdot$ 为普通乘法。证明*对 Δ 是不可分配的。

6.2　二元运算中的特殊元素

6.2.1　幺元

[定义 6-7] 设*是集合 A 上的二元运算。

(1) 若 $\exists e_l\in A$，对 $\forall x\in A$，有 $e_l*x=x$，称 e_l 是运算*的**左幺元**。

(2) 若 $\exists e_r \in A$，对 $\forall x \in A$，有 $x*e_r = x$，称 e_r 是运算*的**右幺元**。

(3) 若 $\exists e \in A$，对 $\forall x \in A$，有 $e*x = x*e = x$，称 e 是运算*的**幺元**（identity element）。

幺元也称为**单位元**。

例如，1 是乘法运算的幺元，0 是加法运算的幺元，$\varnothing$ 是$\cup$运算的幺元，U 是$\cap$运算的幺元。在 $x*y = \max(x,y)$ 运算中，集合的最小元素是幺元，而 $x \circ y = \min(x,y)$ 运算中的集合最大元素是幺元。在 n 阶矩阵中，单位矩阵是乘法幺元，零矩阵是加法幺元。

在一些特殊的运算中，可能只存在左幺元而不存在右幺元，或者相反。

例如，$S = \{a,b,c,d\}$，定义 S 上的两个运算 * 和∘的运算表如表 6-4 和表 6-5。其中，b 和 d 都是 * 的左幺元，a 是∘的右幺元。

表 6-4

*	a	b	c	d
a	d	a	b	c
b	a	b	c	d
c	a	b	c	c
d	a	b	c	d

表 6-5

∘	a	b	c	d
a	a	b	d	c
b	b	a	c	d
c	c	d	a	b
d	d	d	b	c

[辨析] 横看左幺（零、逆）元，竖看右幺（零、逆）元。

[定理 6-1] 如果一个二元运算*的左幺元 e_l 和右幺元 e_r 都存在，则 $e_l = e_r = e$，且幺元是唯一的。

证明 因为 e_l 和 e_r 分别为左、右幺元，则

$$e_l = e_l * e_r = e_r。$$

若 e 和 e' 都是幺元，则

$$e = e*e' = e'。$$

说明幺元是唯一的。

6.2.2 零元

[定义 6-8] 设*是集合 A 上的二元运算。

(1) 若 $\exists \theta_l \in A$，对 $\forall x \in A$，有 $\theta_l * x = \theta_l$，称 θ_l 是运算*的**左零元**。

(2) 若 $\exists \theta_r \in A$，对 $\forall x \in A$，有 $x*\theta_r = \theta_r$，称 θ_r 是运算*的**右零元**。

(3) 若 $\exists \theta \in A$，对 $\forall x \in A$，有 $\theta*x = x*\theta = \theta$，称 θ 是运算*的**零元**（zero element）。

例如，0 是乘法运算的零元，加法运算没有零元。$\varnothing$ 是$\cap$运算的零元，U 是$\cup$运算的零元。在 $x*y = \max(x,y)$ 运算中，集合的最大元素是零元，而 $x \circ y = \min(x,y)$ 运算中的集合最小元素是零元。

类似地，一个运算中可能只存在左零元而不存在右零元，或者相反，如例 6-3 的运算 $a*b = b$ 中，所有元素都是右零元，但没有左零元。

[定理 6-2] 如果一个二元运算*的左零元 θ_l 和右零元 θ_r 都存在，则 $\theta_l = \theta_r = \theta$，且零元是唯一的。

证明 因为 θ_l 和 θ_r 分别为左、右零元，则

$$\theta_l = \theta_l * \theta_r = \theta_r。$$

若 θ 和 θ' 都是零元，则

$$\theta = \theta * \theta' = \theta'。$$

说明零元是唯一的。

[定义 6-9] 对 $\forall x, y, z \in A$，θ 为二元运算*的零元。若 $x \neq \theta$，且 $x*y = x*z$ 或 $y*x = z*x$，必有 $y = z$，则称运算 * 满足**消去律**（cancellation）。

例如，实数集 **R** 上的乘法和整数集 **Z** 上的加法均满足消去律，即若有

$$a \times b = a \times c，或 b \times a = c \times a，且 a \neq 0。$$

必有 $b = c$。

又，若有

$$a + b = a + c，或 b + a = c + a。$$

必有 $b = c$。由于整数集上的加法没有零元，消去律中不必考虑零元的问题。

[辨析] 不要总将*错认为乘法是非常重要的，它只是一种抽象的表示，完全可以是加法。

矩阵乘法不满足消去律。例如，若

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, C = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}, R = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}。$$

虽然 $A \times B = A \times C = R$，且 A 不是乘法零元（零矩阵），但 $B \neq C$。

6.2.3　逆元

[定义 6-10] 设 e 是 A 上二元运算*的幺元，$x \in A$。

(1) 若 $\exists x_l \in A$，使 $x_l * x = e$，称 x_l 为 x 的**左逆元**。

(2) 若 $\exists x_r \in A$，使 $x * x_r = e$，称 x_r 为 x 的**右逆元**。

(3) 若 $\exists \tilde{x} \in A$，使 $\tilde{x} * x = x * \tilde{x} = e$，称 $\tilde{x}$ 为 x 的**逆元**（invertible element）。

显然，如果 $\tilde{x}$ 是 x 的逆元，则 x 也是 $\tilde{x}$ 的逆元，二者互逆。通常，x 的逆元可记作 x^{-1}。

[辨析] 幺元 e 一定存在逆元，就是它自己。幺元也是等幂元，因为 $e^2 = e$。

例如，0 是自然数集 **N** 中加法的幺元，除 0 外，所有元素都没有逆元。对于整数集 **Z**，任何元素 x 都存在加法逆元 $-x$。对于 **R** 上的乘法，除 0 外的所有元素 x 都存在逆元 $1/x$。在 n 阶实数矩阵的乘法中，单位矩阵是幺元，任何可逆矩阵 M 都存在逆元 M^{-1}。

又如，记 $S = \{x \mid x \in \mathbf{Z}$ 且 $m \leqslant x \leqslant n\}$，则在 max 运算中，$m$ 是幺元，且只有 m 有逆元 m。在 C 语言中，将所有字符串集合 Σ^* 上的字符串连接视为运算，则空字符串为幺元，且只有空字符串有逆元。

同样，左、右逆元可能分别存在且不唯一。

[定理 6-3] 设 e 是 A 上二元运算*的幺元，如果 A 的每个元素都有左逆元，且*是可结合的，则 A 的每个元素的左逆元也必定是其右逆元，且每个元素的逆元是唯一的。

证明 对 $\forall a \in A$，设 $b \in A$ 是 a 的左逆元，$c \in A$ 是 b 的左逆元，则

$$a*b = e*(a*b) = (c*b)*(a*b) = c*(b*a)*b = c*e*b = c*b = e。$$

说明 b 是 a 的右逆元。

设 b 和 c 都是 a 的逆元，则

$$b = b*e = b*(a*c) = (b*a)*c = e*c = c。$$

说明逆元是唯一的。

[理解] 这里的结合性很关键。在一般代数系统证明中，可以比照常见运算如乘法、加法分析问题，但必须注意实际的运算所具有的性质，每做一步推理，都要有相应的性质来保证。

[辨析] 定理 6-3 的结果在每个元素都有逆元时成立，部分元素有逆元时可能不成立。

例 6-4 记 $N_k = \{0,1,2,\cdots,k-1\}$，定义 N_k 上的“模 k 加法” $+_k$ 为

$$x +_k y = \begin{cases} x+y & ,x+y<k \\ x+y-k & ,x+y \geqslant k \end{cases}。$$

问是否每个元素都有逆元？

解 0 是幺元，每个元素 x 都有逆元 $k-x$。

[理解] $x +_k y$ 的结果就是 $x+y$ 除以 k 的余数。

思考与练习 6.2

6-7 说明思考与练习 6.1 中第 6-3 和 6-4 题定义的运算是否存在幺元和零元。

6-8 说明思考与练习 6.1 中第 6-3 题定义的运算是否每个元素都有逆元。

6-9 如果一个运算中存在逆元，则每个元素都有逆元，且该元素的逆元是唯一的。这一论断正确吗？

6-10 说明 $n \times n$（$n \geqslant 2$）阶矩阵乘法是否满足消去律。

6-11 设 $A = \{a + b\sqrt{3} \mid a,b \in \mathbf{Q}\}$，$B = \{a + b\sqrt[3]{3} \mid a,b \in \mathbf{Q}\}$，集合 A、B 上的普通乘法存在幺元和零元吗？每个元素都有逆元吗？

6-12 设代数系统<**R**, ⊡>中的二元运算⊡满足：对 $\forall a,b \in \mathbf{R}$，有

$$a \boxdot b = a + b + a \cdot b。$$

证明⊡是可结合的，且 0 是运算的幺元。

6.3 代 数 系 统

6.3.1 代数与子代数

[定义 6-11] 一个非空集合 A 连同其上定义的若干运算 $f_1, f_2, \cdots, f_k$ 组成的系统称为**代数系统**

（algebra system），记作$< A, f_1, f_2, \cdots, f_k >$。代数系统也称为**代数结构**（algebra structure），简称为**代数**。

例如，正整数集合 $\mathbf{Z}^+$及其上的普通加法构成代数系统<$\mathbf{Z}^+$，+>；n 阶实数矩阵集合 M_n 与其上的矩阵乘法和加法构成代数系统<M_n，×，+>；集合 S 的幂集 $\mathscr{P}(S)$及其上的∪、∩和－运算构成了代数系统<$\mathscr{P}(S)$，∪，∩，－>。

一个代数系统的幺元和零元通常起着重要作用，被称为**代数常数**或**特异元素**。可以在代数系统中指明代数常数以强调它们的存在，如<$\mathscr{P}(S)$，∪，∩，－，Ø，U>。

[定义 6-12] 设$< A, f_1, f_2, \cdots, f_k >$是一个代数系统，$B \subseteq A$ 且 $B \neq \varnothing$。若 B 对运算$f_1, f_2, \cdots, f_k$都封闭，且 B 和 A 含有相同的代数常数，则称$< B, f_1, f_2, \cdots, f_k >$为$< A, f_1, f_2, \cdots, f_k >$的**子代数**（subalgebra）。

例如，<**N**，+>是<**Z**，+>的子代数，因为 **N** 对+运算封闭，且二者有相同的幺元 0。但<**N** – {0}，+>不是<**Z**，+>的子代数，因为 **N** – {0}不存在 **Z** 的幺元 0。

例 6-5　对于任意自然数 n，记 $nZ = \{n \cdot i \mid i \in \mathbf{Z}\}$，则$< nZ, + >$是<**Z**，+>的子代数。

证明　因为对任意的 $n \cdot i$ 和 $n \cdot j$，有

$$n \cdot i + n \cdot j = n \cdot (i + j) \in nZ \text{。}$$

即 nZ 对+运算封闭，且它们有共同的幺元 0，故结论成立。

[理解] 子代数与原代数是同类型的代数系统，运算功能也相同，只是范围略小，是原代数的“缩影”。

6.3.2　同态与同构

研究代数系统的重要目的就是探索其共性，以便可以将一种代数系统上的运算转换为另一种代数系统上的其他运算。这里只说明具有一个二元运算的代数系统之间的同态和同构。

[定义 6-13] 设<A, *>和<B, ∘>是代数系统，* 和∘是二元运算。若存在映射 φ：$A \to B$，使对 $\forall x, y \in A$，有

$$\varphi(x*y) = \varphi(x) \circ \varphi(y) \text{。}$$

则称 φ 是<A, *>到<B, ∘>的一个**同态映射**，并称<A, *>和<B, ∘>**同态**（homomorphism），记作 $A \sim B$。称 $\varphi(A)$为<A, *>的**同态像**，也可以直接称 φ 是<A, *>到<B, ∘>的同态。

例 6-6　记 $N_k = \{0,1,2,\cdots,k-1\}$，$+_k$ 为例 6-4 中定义的模 k 加法，则<**N**,+>与<N_k, $+_k$>同态。

证明　构造映射 φ：$\mathbf{N} \to N_k$，使得

$$\varphi(x) = x (\bmod k) \text{。}$$

那么，对 $\forall x, y \in \mathbf{N}$，有整数 m 和 n，使得

$$x = mk + x (\bmod k),\ \ y = nk + y (\bmod k) \text{。}$$

于是，有

$$\begin{aligned} \varphi(x + y) &= (x + y) (\bmod k) \\ &= (mk + x (\bmod k) + nk + y (\bmod k)) (\bmod k) \end{aligned}$$

$$
\begin{aligned}
&= (x(\bmod k) + y(\bmod k))(\bmod k) \\
&= x(\bmod k) +_k y(\bmod k) \\
&= \varphi(x) +_k \varphi(y)。
\end{aligned}
$$

因此，<**N**,+>与<N_k, $+_k$>同态。

[理解] 同态以及下文的同构是指两个代数系统有类似的形态，可以将一个代数系统的运算转换为另一个代数系统上更简单的运算。同态映射可以有多个。

[定义 6-14] 设 φ 是<A, *>到<B, ∘>的同态。若 φ 是满射，则称 φ 是**满同态**；若 φ 是单射，则称 φ 是**单同态**或**单一同态**；若 φ 是双射，则称 φ 是<A, *>到<B, ∘>的**同构**（isomorphism），或称<A, *>与<B, ∘>同构，记作 $A \cong B$。

特别地，$A=B$ 时的同态称为**自同态**，$A=B$ 时的同构称为**自同构**。

例 6-7 证明<$\mathbf{R}^+$, ·>与<**R**,+>同构。

证明 对于代数系统<$\mathbf{R}^+$, ·>和<**R**,+>，构造映射 φ：$\mathbf{R}^+ \to \mathbf{R}$，满足

$$\varphi(x) = \ln x, \quad \forall x \in \mathbf{R}^+。$$

那么，对 $\forall x, y \in \mathbf{R}^+$，有

$$\varphi(x \cdot y) = \ln(x \cdot y) = \ln x + \ln y = \varphi(x) + \varphi(y)。$$

可见，双射 $\ln x$ 是<$\mathbf{R}^+$, ·>到<**R**,+>的同构。

当然，也可以建立<**R**,+>到<$\mathbf{R}^+$, ·>的同构。构造映射 f：$\mathbf{R} \to \mathbf{R}^+$，满足

$$f(x) = \mathrm{e}^x, \quad \forall x \in \mathbf{R}。$$

那么，对 $\forall x, y \in \mathbf{R}$，有

$$f(x+y) = \mathrm{e}^{x+y} = \mathrm{e}^x \cdot \mathrm{e}^y = f(x) \cdot f(y)。$$

可见，双射 e^x 是<**R**,+>到<$\mathbf{R}^+$, ·>的同构。

上述示例说明，$\mathbf{R}^+$上的乘法可以转换为 **R** 上的加法，反之亦然。在一个系统上实现某种计算复杂时，可以转换到另一个系统中进行计算，再将结果通过反函数转换到原系统中。

又如，构造映射 φ：$\mathbf{Z} \to \mathbf{Z}$，满足

$$\varphi(x) = ax, \quad \forall x \in \mathbf{Z}。$$

其中的 $a \in \mathbf{Z}$。若 $a = \pm 1$，则双射 φ 为<**Z**,+>到<**Z**,+>的自同构；若 $a \neq 0$，则 φ 为<**Z**,+>到<**Z**,+>的单自同态，因为 φ 为单射。

[理解] 同构的两个代数系统本质上是相同的，所不同的只是采用的符号有差异。

例 6-8 验证表 6-6～表 6-8 中的三个代数系统<A, *>、<B, ⊕>和<C, ∘>是同构的。

表 6-6

*	a	b
a	a	b
b	b	a

表 6-7

⊕	偶	奇
偶	偶	奇
奇	奇	偶

表 6-8

∘	0°	180°
0°	0°	180°
180°	180°	0°

解　略。

容易验证，若 φ 是代数系统<A,*>到<B, ∘>的同态，*运算的可交换性和可结合性等性质都可在其同态像 $\varphi(A)$中保持下来，其幺元 e 和元素 x 的逆元 x^{-1} 也映射为同态像 $\varphi(A)$的幺元 $\varphi(e)$和逆元 $\varphi(x^{-1})$。

思考与练习 6.3

6-13　两个代数系统之间可能存在多于一个的同态吗？

6-14　若 $<B,*,\Delta>$ 是 $<A,*,\Delta>$ 的子代数，则 $<B,*,\Delta>$ 应满足什么条件？

6-15　对于代数系统 $<\mathbf{Z},\cdot>$，其中的运算 $\cdot$ 为普通乘法。试构造一个集合 S={正、负、零}上的运算 $\odot$ 和一个 $<\mathbf{Z},\cdot>$ 与 $<S,\odot>$ 的同态，以便能够利用 $<S,\odot>$ 得到两个整数相乘结果的符号。

6-16　设 f 是 $<A,*>$ 到 $<B,\Delta>$ 的同态，g 是 $<B,\Delta>$ 到 $<C,\boxdot>$ 的同态，证明 $g\circ f$ 是 $<A,*>$ 到 $<C,\boxdot>$ 的同态。

6-17　设*是集合 G 上的可结合二元运算，且 G 的每个元素都有逆元。构造函数 f：$G\to G$，满足

$$f(x)=x^{-1},\forall x\in G。$$

证明 f 是 G 的自同构当且仅当*是可交换的。

6-18　设*是集合 G 上的可结合二元运算，且 G 的每个元素都有逆元。若 $a\in G$，构造函数 f：$G\to G$，满足

$$f(x)=a*x*a^{-1},\forall x\in G。$$

证明 f 是 G 到 G 的自同构。

6-19　说明代数系统 $<\mathbf{R}-\{0\},\times>$ 与代数系统 $<\mathbf{R},+>$ 不能同构。

6.4　半群与独异点

半群和独异点是两类最简单的单运算代数系统。

[定义 6-15] 设<S,*>为代数系统，$S\neq\varnothing$。若二元运算*是可结合的，称<S,*>为**半群**（semigroup）。如果运算中含有幺元，则称<S,*>为（**含**）**幺半群**或**独异点**（monoid）。如果*运算是可交换的，则称<S,*>为**可交换半群**。

例如，记 $S_k=\{x|\,x\in\mathbf{Z}$ 且 $x\geqslant k\}$，$k\geqslant 0$，则<S_k, +>是半群。这里的 $k\geqslant 0$ 限制很重要。若无此限制，两个负数的和可能小于 k，导致运算不封闭。

代数系统<**N**，−>和<$\mathbf{R}^+$，/>都不是半群。

代数系统<**N**，+>、<**N**，·>、<**R**，·>都是可交换独异点，但<$\mathbf{N}-\{0\}$，+>和<$\mathbf{R}-\{1\}$，·>不是独异点，因为没有幺元。集合 S 的幂集 $\mathscr{P}(S)$上构成的代数系统<$\mathscr{P}(S)$，∪>和<$\mathscr{P}(S)$，∩>是可交

换独异点，$\varnothing$ 和 U 分别是其幺元。由于函数复合运算。满足结合律，故代数系统<S^S，。>是独异点，恒等函数 $I_S(x)$为幺元。

例 6-9 设$\mathcal{A}$是由字符组成的集合，称为字符表。$\mathcal{A}$上的字符串是由其元素组成的字符序列。例如，u=*ababb*，v=*accbaaa* 都是$\mathcal{A}=\{a,b,c\}$ 上的字符串。不含任何字符的字符串 λ 称为空串。定义所有字符串集合上的连接运算⊕，$u\oplus v$ 是由 u 的字符后接 v 的字符组成的字符串，如

$$u\oplus v = ababbaccbaaa。$$

那么，$\mathcal{A}$上的字符串集合 $\sum$ 连同⊕运算构成独异点。

解 因为⊕显然是可结合的且 λ 为幺元，故$<\sum,\oplus>$是独异点。

例 6-10 设 m 是任意正整数，Z_m 是由 $\mathbf{Z}$ 上的模 m 同余类组成的同余类集{[0], [1], [2],…, [m−1]}，在 Z_m 上定义模 m 同余类加法 $\oplus_m$ 和乘法 $\otimes_m$ 如下：

$$[i]\oplus_m[j]=[(i+j)(\mathrm{mod}\ m)],$$

$$[i]\otimes_m[j]=[(i\cdot j)(\mathrm{mod}\ m)]。$$

则<Z_m，$\oplus_m$>和<Z_m，$\otimes_m$>都是独异点。

证明 以下简记$\oplus_m$ 和$\otimes_m$ 为⊕和⊗。

首先，由于运算⊕和⊗的结果都是除 m 后的余数构成的同余类，故运算封闭。

其次，对 $\forall[i],[j],[k]\in Z_m$，记 $i+j=tm+p$，t、p 分别为商和余数，则

$$\begin{aligned}([i]\oplus[j])\oplus[k]&=[(i+j)(\mathrm{mod}\ m)]\oplus[k]=[(p+k)(\mathrm{mod}\ m)]\\&=[(i+j-tm+k)(\mathrm{mod}\ m)]=[(i+j+k)(\mathrm{mod}\ m)]。\end{aligned}$$

同样，$[i]\oplus([j]\oplus[k])=[(i+j+k)(\mathrm{mod}\ m)]$。故⊕是可结合的。

类似地，可以证明⊗也是可结合的。

最后，[0]是⊕的幺元，[1]是⊗的幺元。结论成立。

[理解] 模 m 同余运算可定义为 $[i]\oplus_m[j]=[i+j],[i]\otimes_m[j]=[i\cdot j]$，因为 $[(i+j)(\mathrm{mod}\ m)]=[i+j]$，$[(i\cdot j)(\mathrm{mod}\ m)]=[i\cdot j]$。

例 6-11 设<S,*>是独异点，对 $\forall a,b\in S$，若 a 有逆元，则 $(a^{-1})^{-1}=a$；若 b 也有逆元，则 $(a*b)^{-1}=b^{-1}*a^{-1}$。

证明 因 $a^{-1}*a=a*a^{-1}=e$，故 $(a^{-1})^{-1}=a$。又

$$\begin{aligned}(a*b)*(b^{-1}*a^{-1})&=a*(b*b^{-1})*a^{-1}=a*a^{-1}=e\\&=b^{-1}*e*b=b^{-1}*(a^{-1}*a)*b=(b^{-1}*a^{-1})*(a*b)。\end{aligned}$$

故 $(a*b)^{-1}=b^{-1}*a^{-1}$。结论成立。

[辨析] 这里再次体现了可结合性的重要性。同时，正是因为可结合性的存在，半群中 n 个元素的连续运算 $a_1*a_2*\cdots*a_n$ 可任意加括号而计算结果不变，n 个 a 的连续运算可记为 a^n。

容易想象，因为幺元的存在，独异点的运算表中没有任何两行（或两列）是完全相同的，因为至少与幺元对应位置上的元素是不同的。

[定义 6-16] 设<S,*>为半群，若非空集合 $B \subseteq S$ 且 B 对*运算封闭，则<B,*>也是一个半群，称为<S,*>的**子半群**（sub-semigroup）。

可见，半群的子代数就是子半群。

例如，<[0,1], $\cdot$>是半群<**R**, $\cdot$>的子半群。

思考与练习 6.4

6-20　若<S,*>是半群，运算*必须满足结合律吗？必须满足交换律吗？

6-21　设<S, *>是半群，$a \in S$，定义 S 上的二元运算⊡，使得对 $\forall x, y \in S$，有

$$x \boxdot y = x * a * y。$$

证明<S, ⊡>是半群。

6-22　设 $< A, * >$ 为半群，且对 $\forall x, y \in A$，$x \neq y$，有 $x * y \neq y * x$。证明：

(a) 对 $\forall x \in A$，有 $x * x = x$。　　(b) 对 $\forall x, y \in A$，有 $x * y * x = x$。

(c) 对 $\forall x, y, z \in A$，有 $x * y * z = x * z$。

6-23　设 $< A, * >$ 是可交换半群，若有 $a, b \in A$，$a^2 = a$，$b^2 = b$，则 $(a*b)^2 = a*b$。

6-24　证明有限半群 $< S, * >$ 中一定存在幂等元素，即 $\exists a \in S$，使得 $a^2 = a$。

6.5　群 与 子 群

群是最重要的一类仅含一个二元运算的代数系统。

6.5.1　群的概念

[定义 6-17] 设<G,*>为代数系统，$G \neq \varnothing$。若二元运算*是可结合的，含有幺元 e，且每个元素 x 都有逆元 x^{-1}，则称<G,*>为**群**（group）。为了简单，也可直接称 G 是群。

如果 G 是有限集合则称<G,*>为**有限群**，且称|G|为**群的阶**，否则称为**无限群**。

如果运算*是可交换的，则称<G,*>为（**可**）**交换群**或**阿贝尔**（**Abel**）**群**。

例如，<**R**，+>、<**R** – {0}，$\cdot$>、<$\mathscr{P}(S)$，⊕>等都是群，其中，0、1 和 Ø 为运算的幺元，$x \in \mathbf{R}$ 的逆元为 $-x$，$x \in \mathbf{R} - \{0\}$的逆元为 1/x，$A \in \mathscr{P}(S)$的逆元为 A。它们都是阿贝尔群。

<**R**，$\cdot$>、<**Q**，$\cdot$>、$< M_n, \cdot >$都不是群，因为 **R** 和 **Q** 中的 0 没有逆元，而 M_n 中的奇异矩阵没有逆元。这里的 M_n 仍表示所有 n 阶实数矩阵集合。

例 6-12　记 $A = \{0°, 60°, 120°, 180°, 240°, 300°\}$，对 $\forall a, b \in A$，$a \odot b$ 表示逆时针旋转 a+b 的角度，则<A, ⊙>是群。

证明　对 $\forall a, b \in A$，$a \odot b$ 的值就是(a+b)(mod 360)，可见，运算的封闭性和可结合性都是存在的。0° 是运算的幺元，其逆元为本身，其他元素 a 的逆元为 360° –a。故<A, ⊙>是群，且是阿贝尔群。

例 6-13 记 $G=\{\begin{bmatrix}1&0\\0&1\end{bmatrix},\begin{bmatrix}1&0\\0&-1\end{bmatrix},\begin{bmatrix}-1&0\\0&1\end{bmatrix},\begin{bmatrix}-1&0\\0&-1\end{bmatrix}\}$，则 G 关于矩阵乘法构成群。

证明 容易验证矩阵乘法构成 G 上的二元运算，且因对角矩阵的特点可知运算满足结合律和交换律。$\begin{bmatrix}1&0\\0&1\end{bmatrix}$ 为幺元，所有元素都以自身为逆元。因此，G 是阿贝尔群。

此例中的群 G 是用矩阵及矩阵乘法给出的，更一般的形式可由表 6-9 所示的运算表描述，记为$<K=\{e,a,b,c\}$，$\circ>$，称为“Klien（克莱因）四元群”。

表 6-9

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

利用 Klien 四元群可以解释四次方程能用根式求解的原因。

[定义 6-18] 设<G,*>是群，对 $\forall a\in G$，$\forall n\in \mathbf{Z}$，定义 a 的 n 次幂为

$$a^n=\begin{cases}e & ,n=0\\ a^{n-1}*a & ,n>0\\ (a^{-1})^m & ,n<0\text{且}m=-n\end{cases}。$$

很明显，由于逆元的存在，群中可以定义元素的负整数次幂。

例如，对于加法群<$\mathbf{Z}$,+>，2 的逆元为 -2，有 $2^3=6$，且

$$2^{-3}=(-2)^3=(-2)+(-2)+(-2)=-6。$$

[定义 6-19] 设<G,*>是群，$x\in G$。使得 $x^m=e$ 的最小整数 m 称为元素 x 的**阶数**（element order，也称**周期**），记作 $|x|=m$。此时，称 x 是**有限阶**的元素。若不存在这样的整数则称 x 是**无限阶**的。

例如，Klien 四元群是一个 4 阶群，除幺元外，它的所有元素都是 2 阶的。

[辨析] 群 G 的阶是指 G 的元素个数$|G|$，其元素 x 的阶是使 $x^m=e$ 的最小整数 m。

可以通过下述方法判别一个群是否为阿贝尔群。

[定理 6-4] 设<G,*>是群，则<G,*>是阿贝尔群的充分必要条件是对 $\forall a,b\in G$，有 $(a*b)^2=a^2*b^2$。

证明 若<G,*>是阿贝尔群，则运算是可交换的，有

$$(a*b)^2=(a*b)*(a*b)=a*a*b*b=a^2*b^2。$$

若 $(a*b)^2=a^2*b^2$，即

$$(a*b)^2=a*b*a*b=a*a*b*b。$$

两端分别消去 a 和 b，得 $a*b=b*a$。交换律成立，故<G,*>是阿贝尔群。结论成立。

由定理易知，在阿贝尔群中，有

$$(a*b)^n=a^n*b^n。$$

[辨析] 阿贝尔群中常称*为“加法”，记*为+，并称 x 的逆元为“负元”，记作 $-x$。于是，可记 $y+(-x)=y-x$，并称为二者的差。实数集上的加法群即是如此。

6.5.2　群的性质

由于要求每个元素都有逆元，群存在着明显的无零元特性。

[定理 6-5] 群中不存在零元。

证明　因为零元没有逆元。若群的阶为 1，唯一的一个元素是幺元。

群还有如下性质：

[定理 6-6] 设<G,*>是群，则

(1) 对 $\forall a_1, a_2, \cdots, a_n \in G$，有

$$(a_1 * a_2 * \cdots * a_n)^{-1} = a_n^{-1} * a_{n-1}^{-1} * \cdots * a_1^{-1} 。$$

(2) 指数律成立，即对 $\forall a \in G$，有

$$a^m * a^n = a^{m+n}，\ (a^m)^n = a^{mn} 。$$

(3) 可以解一次方程，即对 $\forall a, b \in G$，必存在唯一的 $x \in G$，使得

$$a * x = b 。$$

(4) 消去律成立，即对 $\forall a, b, c \in G$，若 $a*b = a*c$ 或者 $b*a = c*a$，则必有 $b = c$。

(5) 除了幺元外，不可能存在其他等幂元。

证明　(1) 是例 6-11 的推广。(2) 可由归纳法证明。

(3) 因为 a 有逆元，令 $x = a^{-1} * b$ 即为所求。如果有两个解 x_1 和 x_2 都满足方程，则

$$a * x_1 = a * x_2 。$$

两边同乘以 a^{-1}，由运算的可结合性即得 $x_1 = x_2$。

(4) 两边同乘以 a^{-1}，由运算的可结合性即得。

(5) 若 $\exists a \in G$，使 $a*a = a$。两边同乘以 a^{-1}，由运算的可结合性即得 $a = e$。

6.5.3　子群

[定义 6-20] 设<G,*>是群，S 是 G 的非空子集，若<S,*>也是群，则称<S,*>是<G,*>的**子群**（subgroup）。

显然，<{e},*>和<G,*>都是<G,*>的子群，称为**平凡子群**。其他子群为**非平凡子群**。

例如，<$\mathbf{Z}$,+>是群，令偶数集 $Z_E = \{x \mid x = 2n，\ n \in \mathbf{Z}\}$，则<$Z_E$,+>是<$\mathbf{Z}$,+>的子群。

[辨析] 群的子代数不一定是群，也就不一定是子群。例如，<$\mathbf{R} - \{0\}$, ·>是群，$\mathbf{Z} - \{0\} \subseteq \mathbf{R} - \{0\}$ 且 $\mathbf{Z} - \{0\}$对乘法运算·封闭，但因为整数无乘法逆元，<$\mathbf{Z} - \{0\}$, ·>不是群，自然不是<$\mathbf{R} - \{0\}$, ·>的子群。

[定理 6-7] 设<S,*>是群<G,*>的子群，则<G,*>中的幺元必是<S,*>的幺元。

证明　若 e_S 和 e 分别是<S,*>和<G,*>的幺元。对 $\forall x \in S$，因为 $x \in G$，有

$$e_S * x = x = e * x。$$

在 G 中由消去律即得 $e_S = e$。

[理解] 因为<*S*,*>是群，运算封闭，*x* 在 *S* 中的逆也是在 *G* 中的逆。

除了直接利用群的定义验证子群外，还存在其他一些子群的判定方法。

[定理 6-8] 设<*G*,*>是群，*S* 是 *G* 的非空子集。若 *S* 是有限集，则只要 *S* 对*运算封闭，<*S*,*>就是<*G*,*>的子群。

证明 设 *G* 的幺元为 *e*。对 $\forall x \in S$，只要说明在 *S* 中有幺元 *e* 和 *x* 的逆元。

因为序列 $x, x^2, x^3, \cdots \in S$，且 *S* 为有限集，必存在正整数 *m* 和 *n*，*m*<*n*，使得 $x^m = x^n$。记 $t = n - m$，有

$$x^m = x^m * x^t。$$

在 *G* 中消去 x^m，得

$$x^t = e。$$

因 *S* 对运算封闭，自然有 $x^t \in S$，即 $e \in S$。

如果 $t=1$，则 *x* 本身是幺元，逆为其自身；如果 *t*>1，由 $e = x^t = x^{t-1} * x$ 知，*x* 的逆元为 x^{t-1}。所以，<*S*,*>是<*G*,*>的子群。

[辨析] 此判别方法仅对有限子集 *S* 有效。

例如，Klien 四元群<*G*={*e*,*a*,*b*,*c*}，∘>有 3 个非平凡子群<{*e*,*a*},∘>、<{*e*,*b*},∘>和<{*e*,*c*},∘>，容易验证这 3 个子集对运算∘封闭，因为 $a \circ a = b \circ b = c \circ c = e$。

又如，设 $T = \{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} | a, b \in \mathbf{R} \wedge a, b \neq 0\}$，*为矩阵乘法，则<*T*,*>是群，其幺元为单位矩阵，$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$的逆元为$\begin{bmatrix} 1/a & 0 \\ 0 & 1/b \end{bmatrix}$。容易验证例 6-13 中的 *G* 对*运算封闭，故<*G*,*>是<*T*,*>的子群。

[定理 6-9] 设<*G*,*>是群，*S* 是 *G* 的非空子集，若 *S* 对*运算封闭，且对 $\forall x \in S$，有 $x^{-1} \in S$，则<*S*,*>是<*G*,*>的子群。

证明 对 $\forall x \in S$，由条件，有 $x^{-1} \in S$。因为 *S* 对*运算封闭，有 $e = x * x^{-1} \in S$，故<*S*,*>是<*G*,*>的子群。

[定理 6-10] 设<*G*,*>是群，*S* 是 *G* 的非空子集，若对 $\forall x, y \in S$，有 $x * y^{-1} \in S$，则<*S*,*>是<*G*,*>的子群。

证明 因为 *S* 非空，$\exists x \in S$。由条件，$x * x^{-1} = e \in S$，即 *S* 中存在幺元。

对 $\forall x \in S$，由条件，有 $e * x^{-1} = x^{-1} \in S$，即 *S* 中存在 *x* 的逆元。

对 $\forall x, y \in S$，因为 $y^{-1} \in S$，由条件，有 $x * (y^{-1})^{-1} = x * y \in S$，即 *S* 对*运算封闭。故<*S*,*>是<*G*,*>的子群。

例 6-14 设<*S*,*>和<*T*,*>是群<*G*,*>的子群，则<$S \bigcap T$,*>是<*G*,*>的子群。

证明 对 $\forall x, y \in S \bigcap T$，有 $x, y \in S$，且 $x, y \in T$。因为<*S*,*>和<*T*,*>是群，知 $y^{-1} \in S$，且 $y^{-1} \in T$。由运算的封闭性，得知 $x * y^{-1} \in S$ 且 $x * y^{-1} \in T$，即 $x * y^{-1} \in S \bigcap T$。结论成立。

上述结论还可以利用定理 6-9 证明如下：

对 $\forall x,y\in S\bigcap T$，有 $x,y\in S$，且 $x,y\in T$。由子群对运算的封闭性，有 $x*y\in S$，且 $x*y\in T$，即 $x*y\in S\bigcap T$，可见 $S\bigcap T$ 对运算*封闭。

对 $\forall x\in S\bigcap T$，则 $x\in S$，且 $x\in T$。因为 S 和 T 是群，有 $x^{-1}\in S$ 且 $x^{-1}\in T$。因此，$x^{-1}\in S\bigcap T$。结论成立。

[辨析] 例 6-14 的后一种证明方法中，第一部分恰好说明了两个子半群的交是子半群。

[延伸] 群论是 19 世纪最具重大意义的数学创造之一，开创了全新的数学领域，它得益于法国的天才数学家伽洛瓦（Évariste Galois）等人的创造性工作。群也是现代数学中最重要和最具概括性的概念之一，它起源于高次代数方程的求解问题，并成功地给出了 5 阶及以上代数方程没有根式解等基本结论[32-34]。

思考与练习 6.5

6-25　半群与群的差别有哪些？

6-26　“群中不能有零元。”是正确的说法吗？为什么？

6-27　设有 $\mathcal{F}=\{f_1,f_2,f_3,f_4,f_5,f_6\}$ 为 $\mathbf{R}-\{0,1\}$ 上的函数集合，各函数定义如下：

$$f_1(x)=x,\quad f_2(x)=x^{-1},\quad f_3(x)=1-x,$$

$$f_4(x)=(1-x)^{-1},\quad f_5(x)=(x-1)x^{-1},\quad f_6(x)=x(x-1)^{-1}。$$

证明 $<\mathcal{F},\circ>$ 是群，其中的$\circ$为函数复合运算。

6-28　设半群 $<G,*>$ 中存在左幺元 e，且对 $\forall x\in G$，有 $\tilde{x}\in G$，使得 $\tilde{x}*x=e$。证明：

(a) 对 $\forall a,b,c\in G$，若 $a*b=a*c$，则 $b=c$。

(b) e 是幺元，且 $<G,*>$ 是群。

6-29　设 $<G,*>$ 是群，对 $\forall a\in G$，定义 $H=\{y\mid a*y=y*a,y\in G\}$，证明 $<H,*>$ 是 $<G,*>$ 的子群。

6-30　设 $<G,*>$ 是群，且 G 有偶数个元素，证明 G 中存在元素 $a\neq e$，但 $a^2=e$，这里的 e 为幺元。

6-31　设 $<G,*>$ 是独异点，且对 $\forall a\in G$，有 $a^2=e$。证明 $<G,*>$ 是阿贝尔群。

6-32　证明任何不超过 4 阶的群都是阿贝尔群。

6-33　若 $<G,*>$ 是有限半群，且运算*满足消去律，证明 $<G,*>$ 是群。

6-34　若 $<G,*>$ 是群，定义 G 上的二元关系 R 为

$$R=\{<x,y>\mid\exists u(u\in G\wedge y=u*x*u^{-1})\}。$$

证明 R 是 G 上的等价关系。

6-35　设 $<H,*>$ 是 $<G,*>$ 的子群，定义集合 S 为

$$S=\{x\mid x\in G\wedge x*H*x^{-1}=H\}。$$

其中的 $x*H*x^{-1}=\{x*h*x^{-1}\mid h\in H\}$。证明 $<S,*>$ 是 $<G,*>$ 的子群。

6-36 设<G,*>是群，对 $\forall a,b\in G$，证明：

(a) $|a^{-1}|=|a|$。 (b) $|a*b|=|b*a|$。

6.6 循环群与置换群

6.6.1 循环群

[定义 6-21] 设<G,*>是群，若 $\exists a\in G$ 使得 $G=\{a^k \mid k\in \mathbf{Z}\}$，则称 G 为**循环群**（cyclic group），简记为 $G=<a>$。元素 a 称为 G 的**生成元**（generator），称 G 是由 a 生成的群。

例如，例 6-12 中的群$<A=\{0^\circ, 60^\circ, 120^\circ, 180^\circ, 240^\circ, 300^\circ\}, \odot>$是一个有限循环群，其中，$60^\circ$ 是其生成元，0° 为幺元。任何元素都可以表示为 60° 的幂。例如，$180^\circ=(60^\circ)^3$，$0^\circ=(60^\circ)^6=(60^\circ)^{|A|}$。

类似地，可以验证 300° 也是该群的生成元。

例 6-15 证明<$\mathbf{Z}$,+>是无限循环群。

证明 因为 0 是幺元，1 是其生成元，1 的加法逆元 $1^{-1}=-1$。具体说，由指数定义，有 1^0=0。对任意的正整数 m，有

$$m=1^m=\overbrace{1+1+\cdots+1}^{m个}。$$

对于任意的负整数 $-m$，有

$$-m=1^{-m}=(-1)^m=\overbrace{(-1)+(-1)+\cdots+(-1)}^{m个}。$$

可见，所有整数都是由 1 生成的。

类似地，可以说明 –1 也是<$\mathbf{Z}$,+>的生成元。

例 6-16 记 $N_k=\{0,1,2,\cdots,k-1\}$，证明<N_k, $+_k$>为 k 阶循环群，其中的 $+_k$ 为模 k 加法。

证明 0 显然是幺元。因为 $1^0=0$，且对 $\forall m\in N_k$，有

$$m=1^m=\overbrace{1+_k 1+_k\cdots+_k 1}^{m个}。$$

故<N_k, $+_k$>为由 1 生成的 k 阶循环群。

[定理 6-11] 设<G,*>是由元素 a 生成的有限循环群。若 $|G|=n$，则必有 $a^n=e$，即 a 的阶 $|a|=n$，且 $G=\{a,a^2,a^3,\cdots,a^{n-1},a^n=e\}$。

证明 若有 $m<n$，使 $a^m=e$，则 $|G|<n$。这是因为，对 $\forall a^k\in G$，记 $k=qm+r$，$0\leqslant r<m$，有

$$a^k=a^{qm+r}=a^{qm}*a^r=(a^m)^q*a^r=a^r。$$

这说明 G 至多有 m 个元素，与 $|G|=n$ 矛盾。

此外，$a,a^2,a^3,\cdots,a^{n-1},a^n$ 互不相同，否则，若有 $0\leqslant i<j\leqslant n$，使

$$a^i = a^j。$$

于是，有 $a^{j-i} = e$。由于 $j-i<n$，已证明是不可能的。因此，必有 $G = \{a, a^2, a^3, \cdots, a^{n-1}, a^n = e\}$。

[定理 6-12] 循环群一定是阿贝尔群。

证明　设 a 为循环群 G 的生成元。对 $\forall a^m, a^n \in G$，有

$$a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m。$$

故 G 是阿贝尔群。

应注意循环群的生成元可能不是唯一的。例如，表 6-10 显示了一个群<G,*>的运算表，其中的 e 为幺元。因为

$$b^2 = a,\ b^3 = c,\ b^4 = e,$$
$$c^2 = a,\ c^3 = b,\ c^4 = e。$$

可见，b 和 c 都是 G 的生成元。

表 6-10

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

6.6.2　置换群

1．n 元置换与置换群

[定义 6-22] 设 $S = \{1,2,\cdots,n\}$，任意的双射 σ：$S \to S$ 构成 S 上 n 个元素的置换，称为 ***n* 元（阶）置换**（permutation），记作

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \vdots & \sigma(n) \end{pmatrix}。$$

例如，设 $S = \{1,2\}$，则 S 上有两个 2 元置换：

$$\sigma_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix},\ \sigma_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}。$$

由于 n 个元素有 $n!$种排列，故 $S = \{1,2,\cdots,n\}$上有 $n!$个 n 元置换，所有这些置换组成的集合记作 S_n，即

$$S_n = \{\ \sigma \mid \sigma \text{ 为 } S \text{ 上的 } n \text{ 元置换}\}。$$

[定义 6-23] 设 σ 和 τ 是 $S = \{1,2,\cdots,n\}$的 n 元置换，则 σ 与 τ 的复合 $\sigma \circ \tau$ 表示先对 S 的元素进行 τ 置换再进行 σ 置换，则 $\sigma \circ \tau$ 也是 S 上的 n 元置换，称为 **σ 与 τ 的乘积**，简记为 $\sigma\tau$。

[理解] 一个 n 元置换就是一个由 S 到 S 的双射，σ 与 τ 的复合 $\sigma \circ \tau$ 就是函数的（左）复合。

例如，$S = \{1,2,3,4,5\}$，以下是两个 5 元置换与其乘积：

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix},\ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix},$$

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix},\ \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix}。$$

因为 $\sigma\tau$ 表示函数 σ 与 τ 的复合，为 S 到 S 的函数。对 $\forall x \in S$，有

$$\sigma\tau(x) = \sigma(\tau(x))。$$

对部分元素执行 $\sigma\tau$ 置换的过程如下：

$$1 \xrightarrow{\tau} 4 \xrightarrow{\sigma} 1，\ 即 1 \xrightarrow{\sigma\tau} 1;$$

$$2 \xrightarrow{\tau} 3 \xrightarrow{\sigma} 2，\ 即 2 \xrightarrow{\sigma\tau} 2;$$

$$3 \xrightarrow{\tau} 1 \xrightarrow{\sigma} 5，\ 即 3 \xrightarrow{\sigma\tau} 5。$$

由于 σ 、 τ 是双射，故 $\sigma\tau$：$S \to S$ 仍为 S 上的双射函数。将置换的复合表示为乘积仅是一种更为简洁的表示方法，运算仍为复合运算∘，也称为**置换乘法**。

[定理 6-13] $<S_n, \circ>$ 构成一个群，称为集合 S 的 ***n* 元（次）对称群**（symmetric group）。

证明 S_n 关于置换乘法∘是封闭的。函数复合运算本身满足结合律，恒等置换 σ_e（即恒等函数 I_S）是 S_n 的幺元（称为**幺置换**）。对于任何 n 元置换 σ，其逆函数是 σ 的逆元（称为**逆置换**）。

[定义 6-24] $<S_n, \circ>$ 的任何一个子群称为集合 S 上的一个 n 元（次）**置换群**（permutation group）。

[辨析] 显然，$<S_n, \circ>$ 也是集合 S 的置换群，只是它还有个特殊的名字叫对称群。

例 6-17 设 $S = \{1,2,3\}$，写出 S 的对称群和 S 上的置换群。

解 S 的对称群为 $<S_3, \circ>$，其中，$S_3 = \{\sigma_e, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$，有

$$\sigma_e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}。$$

S_n 上的置换乘法如表 6-11 所示。

表 6-11

∘	σ_e	σ_1	σ_2	σ_3	σ_4	σ_5
σ_e	σ_e	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_1	σ_e	σ_5	σ_4	σ_3	σ_2
σ_2	σ_2	σ_4	σ_e	σ_5	σ_1	σ_3
σ_3	σ_3	σ_5	σ_4	σ_e	σ_2	σ_1
σ_4	σ_4	σ_2	σ_3	σ_1	σ_5	σ_e
σ_5	σ_5	σ_3	σ_1	σ_2	σ_e	σ_4

因为$<\{\sigma_e, \sigma_1\}, \circ>$、$<\{\sigma_e, \sigma_2\}, \circ>$、$<\{\sigma_e, \sigma_3\}, \circ>$和$<\{\sigma_e, \sigma_4, \sigma_5\}, \circ>$都是 $<S_3, \circ>$ 的子群，故它们都是 S 上的置换群。当然，$<\{\sigma_e\}, \circ>$和 $<S_3, \circ>$ 也是 S 上的置换群。

2．置换的轮换表示

n 元置换可以采用轮换的积来简化表示。

[定义 6-25] 设 σ 是 $S=\{1,2,\cdots,n\}$的 n 元置换，若

$$\sigma(i_1)=i_2,\sigma(i_2)=i_3,\cdots,\sigma(i_{k-1})=i_k,\sigma(i_k)=i_1$$

且保持 S 中的其他元素不变，则称 σ 是 S 上的 ***k* 阶轮换**，记作 $(i_1,i_2,\cdots,i_k)$。特别地，如 k=2，称 σ 是 S 上的**对换**。

例如，例 6-17 中 S_3 的各置换可以用轮换表示为：

$$\sigma_e=(1),\ \sigma_1=(1,2),\ \sigma_2=(1,3),\ \sigma_3=(2,3),\ \sigma_4=(1,2,3),\ \sigma_5=(1,3,2)。$$

其中的 σ_1、σ_2 和 σ_3 都是对换。

又如，以下是一个 6 元置换，它被表示成一个对换和 3 阶轮换的积：

$$\sigma=\begin{pmatrix}1&2&3&4&5&6\\2&1&3&6&4&5\end{pmatrix}=(1,2)(4,6,7)。$$

[辨析] 轮换是在几个元素之间完成一个“小循环”；将 a 变成 b 并将 b 变成 a 的 2 阶轮换是直接将 a 和 b 对换；阶数为 1 的轮换是自身到自身的变换，在乘积中一般不写，即置换(1)(3)(2,4)与(1)(2,4)、(3)(2,4)和(2,4)是等同的。

可以说明，任何 n 元置换均可以分解为不相交的轮换的积。

置换群在具有对称结构的离散系统中具有重要的应用。

[延伸] 置换群是最早被研究的群，在解决对称问题及计数等方面具有直接应用。置换群的重要性还体现在，任何一个有限群都与某个置换群同构，也可以理解为一个有限群总可以用一个置换群表示出来[33-36]。

思考与练习 6.6

6-37　“循环群有唯一的生成元。”是正确的说法吗？

6-38　证明循环群的子群也是循环群。

6-39　设 $G=<a>$是循环群，证明：

(a) 若 G 是无限群，则 G 的生成元是 a 和 a^{-1}。

(b) 若 $|G|=n$，对任意的正整数 r，若 r 与 n 互质（最大公约数为 1，记为 $(n,r)=1$），则 a^r 是 G 的生成元。

6-40　找出$<N_6,+_6>$、$<N_7,+_7>$和$<N_{12},+_{12}>$的所有生成元。

6-41　设 $G=<a>$是循环群，$\mathbf{Z}$ 和 Z_n 分别为整数加法群和同余类加法群。证明：如果 $|a|=+\infty$，则 $G\cong\mathbf{Z}$；如果 $|a|=n$，则 $G\cong Z_n$。

6-42　将 S={1,2,3,4}上的下列置换写成不相交轮换的积。

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}。$$

6-43　验证 $S=\{1,2,3\}$上的置换集合{(1),(1,2,3)}和{(1),(1,2),(3),(1,2,3),(1,3,2)}关于置换的复合运算不能构成群。

6-44 将一个 2×2 棋盘的每个格子涂成黑色，棋盘的旋转和翻转均是对原始排列的置换，且保持棋盘状态不变。写出所有的置换，并验证所有置换组成的集合 G 关于置换的复合运算构成群。

6.7 群的陪集分解

可以利用子群产生陪集，进而对群进行分解，实现对原集合的划分。

6.7.1 陪集

先观察一下同余类的例子。这里利用[i]表示整数集 **Z** 上的模 3 同余关系产生的同余类，那么，**Z** 共有 3 个不同的同余类[0]、[1]和[2]。对于群<**Z**,+>，易知<[0],+>是<**Z**,+>的子群，0 是幺元。对 $\forall i\in \mathbf{Z}$，如果引入记号：

$$i[0]=\{i+m|m\in[0]\}。$$

那么，**Z** 上的所有同余类可表示为

$$0[0]=[0]，\ 1[0]=[1]，\ 2[0]=[2]。$$

一般地，有

$$i[0]=[i\ (\mathrm{mod}\ 3)]。$$

这说明，所有 i[0]中只有 3 个不同的子集，且其中之一为[0]本身。它们构成了原集合 **Z** 的一个划分。

[定义 6-26] 设<H,*>是群<G,*>的子群，对 $\forall a\in G$，定义

$$aH=\{a*h|h\in H\}$$

为由 a 确定的 H 在 G 中的**左陪集**（left coset）。元素 a 称为陪集 aH 的**代表元素**。

[理解] aH 是由 a 与 H 的所有元素“相乘”构成的集合，也可类似地定义右陪集 Ha。

显然，前文中的 i[0]就是由 i 确定的子群[0]在 **Z** 中的左陪集。

观察 Klien 四元群，$H=\{e,a\}$是 $K=\{e,a,b,c\}$的子群，有

$$eH=aH=H=\{e,a\}，\ bH=cH=\{b,c\}。$$

可见，H 在 K 中只有 2 个不同的左陪集，且它们构成集合 K 的划分。

又如，设 $G=\mathbf{R}\times\mathbf{R}$，则 G 是由平面上所有点组成的集合。G 上的+运算定义为：

$$<x_1,y_1>+<x_2,y_2>=<x_1+x_2,y_1+y_2>。$$

显然，<G,+>是一个具有幺元<0,0>的阿贝尔群。

设 $H=\{<x,y>|\ y=x\}$，则<H,+>构成<G,+>的子群。

那么，H 的陪集又是什么呢？

观察图 6-1 可知，H 是过坐标原点的一条直线，任何一个陪集<x_0,y_0>H 就是对 H 的一次平移，是过<x_0,y_0>点的直线。显然，平面被所有直线划分开，即所有陪集构成平面的一个划分。事实上，H 可以是过原点的具有任何斜率的一条直线。

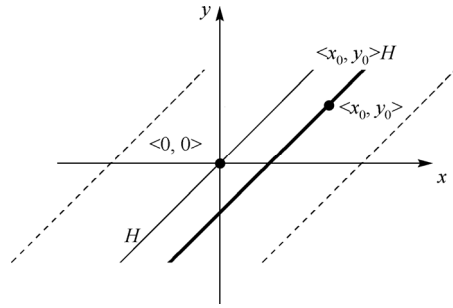


图 6-1

[辨析] H 本身也是一个左陪集，即 eH。因为 $e\in H$，对 $\forall a\in G$，有 $a=a*e\in aH$，这说明 G 的元素 a 总属于 a 产生的左陪集。

从陪集的定义和示例容易得出如下结论：

[定理 6-14] 设<H,*>是群<G,*>的一个子群，则

(1) 对 $\forall a\in G$，有 $aH\neq\varnothing$。

(2) 任意的两个陪集，要么完全重合，要么不相交，即对 $\forall a,b\in G$，若 $aH\neq bH$，则 $aH\cap bH=\varnothing$。

(3) $\bigcup_{a\in G}aH=G$。

证明

(1) 因为幺元 $e\in H$，有 $a=a*e\in aH$，即 $aH\neq\varnothing$。

(2) 等同于证明，若 $aH\cap bH\neq\varnothing$，必有 $aH=bH$。

因为 $aH\cap bH\neq\varnothing$，则 $\exists c\in aH\cap bH$。于是，$\exists h_1,h_2\in H$，使 $c=a*h_1=b*h_2$，这说明 a 与 b 可相互表示，即 $a=b*h_2*h_1^{-1}$，且 $b=a*h_1*h_2^{-1}$。

对 $\forall x\in aH$，$\exists h\in H$，使

$$x=a*h=(b*h_2*h_1^{-1})*h=b*(h_2*h_1^{-1}*h)\in bH\ 。$$

有 $aH\subseteq bH$。同理，$bH\subseteq aH$。故 $aH=bH$。

(3) $\bigcup_{a\in G}aH\subseteq G$ 是自然的。同时，对 $\forall x\in G$，有

$$x\in xH。$$

即 $x\in\bigcup_{a\in G}aH$，故 $G\subseteq\bigcup_{a\in G}aH$。等式成立。

上述定理说明，由子群 H 的所有左陪集构成群 G 的划分。

实际上，a、b 属于同一个左陪集还可以等价地描述成 $a^{-1}*b\in H$。

例 6-18　设<H,*>是群<G,*>的子群，对 $\forall a,b\in G$，$a^{-1}*b\in H$ 当且仅当 $aH=bH$。

证明　$a^{-1}*b\in H\vdash aH=bH$。因为 $a^{-1}*b\in H$，有 $h\in H$，使

$$a^{-1}*b=h。$$

于是，有 $b=a*h\in aH$。又因为 $b\in bH$，即 $b\in aH\cap bH$，说明 aH 与 bH 相交，由定理 6-14 得 $aH=bH$。

$aH=bH\vdash a^{-1}*b\in H$。因为 $aH=bH$，故 $\exists h\in H$，使

$$a=a*e=b*h。$$

于是，$a^{-1}*b=h^{-1}*b^{-1}*b=h^{-1}\in H$。

6.7.2　拉格朗日定理

在群中，因为逆元的存在，容易想象，对 $\forall a\in G$ 和 $\forall h_1,h_2\in H$，$h_1=h_2$ 与 $a*h_1=a*h_2$ 是等价的说法，而这意味着子群 H 与其左陪集 aH 具有相同的基数。

[定理 6-15] 若<H,*>是群<G,*>的一个子群，则

(1) 对 $\forall a \in G$，有 $|aH| = |H|$。

(2) 若 G 是有限群，且 $|G| = n$，$|H| = m$，则 $m | n$，即 m 整除 n。

此定理称为**拉格朗日（Lagrange）定理**。

证明

(1) $\forall a \in G$，构造映射 f：$H \to aH$，使对 $\forall h \in H$，有

$$f(h) = a * h。$$

那么，对 $\forall h_1, h_2 \in H$，若 $f(h_1) = f(h_2)$，即 $a*h_1 = a*h_2$，有 $h_1 = h_2$，这说明 f 是单射。

对 $\forall y \in aH$，必有 $h \in H$，使 $y = a*h = f(h)$，说明 f 是满射。故 f 是双射，结论成立。

(2) 由定理 6-14，G 可被划分为有限个且个数与|H|相等的部分，故 $|H|$ 必能整除 $|G|$。

由拉格朗日定理可以直接得到如下推论：

[定理 6-16] 任何质数阶群不存在非平凡子群。

证明 因为子群的阶必须是原群阶数的因子，而质数除了 1 和自身之外没有其他因子。

[定理 6-17] 设<G,*>是 n 阶有限群，对 $\forall a \in G$，若 $|a| = r$，则必有 $r | n$，且 $a^n = e$。特别地，质数阶群<G,*>必定是循环群，且非幺元的任何一个元素都是生成元。

证明 记 $H = \{a, a^2, a^3, \cdots, a^{r-1}, a^r = e\}$，<$H$,*>显然是<$G$,*>的循环子群。由拉格朗日定理，有 $r | n$。于是，有整数 m 使得 $n = mr$，故 $a^n = a^{mr} = (a^r)^m = e$。

若 n 为质数，<G,*>只能有平凡子群，即 $r = 1$ 或 $r = n$。故<G,*>必是循环群且 $G = < a >$。

[辨析] r=1 意味着只能是由一个元素（幺元）组成的群，自然是循环群。

[延伸] 拉格朗日定理有不同的表述形式，也提供了利用群进行集合元素分类的一种特殊的方法，将这些内容联系在一起学习有助于对问题的理解[37]。

[延伸] 由于有一定抽象性，各种符号也比较多，透彻理解代数系统部分的内容有一定难度，但这些理论并不是符号的堆砌，相反，正是这些理论保证了解决工程问题的能行性，我们也可以直接说明它们在计算机领域的工程应用[38]。

思考与练习 6.7

6-45 设 $Z_6 = \{[0],[1],[2],[3],[4],[5]\}$，运算 $+_6$ 为 Z_6 上的模 6 加法，写出群<Z_6, $+_6$>的幺元、所有元素的逆元、所有子群及其左陪集。

6-46 设 $G = \{f \mid f: \mathbf{R} \to \mathbf{R}, f(x) = ax + b, 且 a, b \in \mathbf{R}, a \neq 0\}$，$\circ$为函数复合运算。

(a) 证明 $< G, \circ >$ 是群。

(b) 设 $S = \{f \mid f \in G 且 a = 1\}$，$T = \{f \mid f \in G 且 b = 0\}$，证明 $< S, \circ >$ 和 $< T, \circ >$ 都是 $< G, \circ >$ 的子群。

(c) 写出 S 和 T 在 G 中的所有左陪集。

6-47 证明任何不超过 5 阶的群都是阿贝尔群。

6-48 证明任何一个 4 阶群只可能是循环群或 Klein 群。

6-49 证明群<G,*>的任一子群<H,*>所确定的左陪集中，只有一个是子群。

第 7 章　环、域、格和布尔代数

常用的代数系统包含两个甚至更多个运算。典型地，考虑实数集 **R** 上的加法+和乘法$\cdot$，它们构成了一个最基本的代数系统<**R**,+,$\cdot$>。很多代数系统<A,+,$\cdot$>都具有类似的结构，只是运算的对象以及运算本身都更为一般，但表现出来的性质与<**R**,+,$\cdot$>类似，所以习惯上仍称这样的系统<A,+,$\cdot$>中的两个运算为加法和乘法。

7.1　环　和　域

7.1.1　环

[定义 7-1] 设<A,+,$\cdot$>是一个代数系统，+和$\cdot$是二元运算。若

(1) <A,+>是阿贝尔群；

(2) <A,$\cdot$>是半群；

(3) 运算$\cdot$对运算+是可分配的。则称<A,+,$\cdot$>是一个**环**（ring）。

例如，整数集、有理数集、实数集和复数集关于普通的加法和乘法构成环，一般称为整数环 **Z**、有理数环 **Q**、实数环 **R** 和复数环 **C**。

若 $n\geqslant 2$，则 n 阶实系数多项式的加法和乘法构成多项式环，n 阶实矩阵的加法和乘法构成矩阵环，$N_n=\{0,1,2,\cdots,n-1\}$上的模 n 加法运算 $+_n$ 和乘法运算 $\times_n$ 构成模 n 整数环。

为了理解和叙述上的方便，一般将环中加法的幺元记作 0 或θ，乘法的幺元记作 1（如果存在）。对任意的元素 x，其加法逆元称为“负元”，记作 $-x$，且将 $x+(-y)$ 写作 $x-y$。

环具有如下性质：

[定理 7-1] 设<A,+,$\cdot$>是一个环，则对 $\forall a,b,c\in A$，有

(1) $a\cdot 0=0\cdot a=0$。　　(2) $a\cdot(-b)=(-a)\cdot b=-(a\cdot b)$。

(3) $(-a)\cdot(-b)=a\cdot b$。　　(4) $a\cdot(b-c)=a\cdot b-a\cdot c$。

(5) $(b-c)\cdot a=b\cdot a-c\cdot a$。

证明

(1) $a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0$，因<$A$,+>是群，消去 $a\cdot 0$，得 $a\cdot 0=0$。

(2) $a\cdot b+a\cdot(-b)=a\cdot(b-b)=a\cdot 0=0$，故 $a\cdot(-b)$ 为 $a\cdot b$ 的负元 $-(a\cdot b)$。同理，$(-a)\cdot b$ 也是 $a\cdot b$ 的负元。

(3) 因 $a\cdot(-b)=-(a\cdot b)$，知 $a\cdot b=-(a\cdot(-b))$。又因为 $(-a)\cdot b=-(a\cdot b)$，有 $(-a)\cdot(-b)=-(a\cdot(-b))$。故 $a\cdot b=(-a)\cdot(-b)$。

(4) $a\cdot(b-c)=a\cdot(b+(-c))=a\cdot b+a\cdot(-c)=a\cdot b-a\cdot c$。

(5) 与(4)类似。

[辨析] 环中加法的幺元 0 恰好是乘法的零元。环中的算律除了乘法不能使用交换律外，其他均与实数的加法和乘法算律相同。

例 7-1 在环中计算 $(a+b)^2$ 和 $(a-b)^2$。

解 $(a+b)^2=(a+b)\cdot(a+b)=a^2+a\cdot b+b\cdot a+b^2$，

$(a-b)^2=(a-b)\cdot(a-b)=a^2-a\cdot b-b\cdot a+b^2$。

[定义 7-2] 在环<A,+, ·>中，若 $a\neq 0$，且 $b\neq 0$，但 $a\cdot b$=0，则称 a 和 b 为**零因子**。

由定义，系统<A,+, ·>无零因子是指，对 $\forall a,b\in A$，若 $a\cdot b=0$，则有 $a=0$ 或 $b=0$。

例如，在 2 阶矩阵环中，$\begin{bmatrix}0&0\\0&0\end{bmatrix}$ 为加法幺元。$\begin{bmatrix}1&0\\0&0\end{bmatrix}$ 和 $\begin{bmatrix}0&0\\0&1\end{bmatrix}$ 均为非加法幺元，但 $\begin{bmatrix}1&0\\0&0\end{bmatrix}\times\begin{bmatrix}0&0\\0&1\end{bmatrix}=\begin{bmatrix}0&0\\0&0\end{bmatrix}$。它们都是零因子。

[延伸] 零因子可严格区分为*左零因子*和*右零因子*。

[定义 7-3] 设<A,+, ·>是环。如果乘法运算 · 是可交换的，则称 A 为**交换环**。如果乘法运算 · 含有幺元，则称 A 为**含幺环**。如果乘法运算无零因子，则称 A 为**无零因子环**。无零因子的含幺交换环称为**整环**（domain）。

显然，<**R**,+, ·>、<$\mathscr{P}(S),\cup,\cap$>和<$\mathscr{P}(S),\oplus,\cap$>都是含幺交换环，但只有<**R**,+, ·>是整环。因为 $\varnothing$ 为加法 $\cup$ 和 $\oplus$ 的幺元，$A=\{a\}\neq\varnothing$ 和 $B=\{b\}\neq\varnothing$，但 $A\cap B=\varnothing$，即它们都是零因子，说明代数系统<$\mathscr{P}(S),\cup,\cap$>和<$\mathscr{P}(S),\oplus,\cap$>都含有零因子，不是整环。

例 7-2 试说明<$N_m=\{0,1,2,\cdots,m-1\},+_m,\times_m$>为何种环。

解 因为 1 是乘法 $\times_m$ 的幺元，且 $\times_m$ 满足交换律，故<$N_m,+_m,\times_m$>为含幺交换环。

若 m 为质数，则不存在 a 和 b，使 $a\cdot b=m$。因此，对 $\forall a\neq 0$ 和 $b\neq 0$，必有 $a\times_m b=(a\cdot b)(\mathrm{mod}\ m)\neq 0$，这说明乘法无零因子，故<$N_m,+_m,\times_m$>为整环。

由于<$Z_m,\oplus_m,\otimes_m$>与<$N_m,+_m,\times_m$>具有相同的性质，自然也构成环，称为“模 m 同余类环”或“模 m 剩余类环”。特别地，当 m 为质数时，<$Z_m,\oplus_m,\otimes_m$>为整环。

实际上，整环中的无零因子等价于乘法消去律。这是因为，若无零因子，且 $a\cdot b=a\cdot c$，则 $a\cdot(b-c)=0$，必有 $b-c=0$，即 $b=c$，说明消去律成立。反之，若存在消去律，且 $a\cdot b=0$。因为 $0=a\cdot 0=0\cdot b$，即 $a\cdot b=a\cdot 0=0\cdot b$。分别消去 a 和 b，即得 $b=0$，$a=0$，可见系统中无零因子。

整环与域已经非常接近，但还不能保证每个元素都有乘法逆元。

7.1.2 域

[定义 7-4] 设<A,+, ·>是一个代数系统。若

(1) <A,+>是阿贝尔群；

(2) <$A-\{0\}$, ·>是阿贝尔群；

(3) 运算·对运算+是可分配的。则称<A,+, ·>是一个**域**（field）。

例如，<**Q**,+, ·>、<**R**,+, ·>和<**C**,+, ·>都是域。不过，<**Z**,+, ·>是整环，但不是域，因为一般的整数 x 没有乘法逆元，即 $1/x \notin \mathbf{Z}$，故<$\mathbf{Z}-\{0\}$, ·>不是阿贝尔群。

显然，域一定是整环，因为（乘法）群中存在消去律，即无零因子，但整环不一定是域。

[定理 7-2] 有限整环一定是域。

证明　设<A,+, ·>是一个有限整环。对 $\forall x \in A$ 且 $x \neq 0$，由运算的封闭性，有陪集 $xA \subseteq A$。因为消去律存在，对 $\forall a,b \in A$ 且 $a \neq b$，必有

$$x \cdot a \neq x \cdot b \text{。}$$

说明 xA 的元素各不相同，从而有 $|xA| = |A|$，故 $xA = A$。

又因为 $1 \in A$，即 $1 \in xA$，故必有 $y \in A$，使得 $x \cdot y = 1$，这说明 y 是 x 的逆元。因此，<$A-\{0\}$, ·>是阿贝尔群，即<A,+, ·>为域。

例 7-3　设 S 为下列集合，+和 · 是普通加法和乘法，判断代数系统<S,+, ·>是否为域。

(a) $S = \{a+b\sqrt{3} \mid a,b \in \mathbf{Z}\}$。　　(b) $S = \{a+b\sqrt{5} \mid a,b \in \mathbf{Q}\}$。

(c) $S = \{a+b\sqrt[3]{5} \mid a,b \in \mathbf{Q}\}$。　　(d) $S = \{4n \mid n \in \mathbf{Z}\}$。

解　(a) 不是域，仅是整环，如 $\sqrt{3}$ 没有逆元。

(b) 是域。$a+b\sqrt{5}$ 的逆元为 $a/(a^2-5b)-[b/(a^2-5b)]\sqrt{5} = a'+b'\sqrt{5}$。

(c) 不是域，仅是整环，如 $\sqrt[3]{5}$ 没有逆元。

(d) 不是域，不是整环，因为 $1 \notin S$，没有乘法幺元。

生活中常见的域主要是“数域”，如实数域、有理数域等，都是无限域，但在计算机科学中，有限域具有特殊的作用。当 m 为质数时，<$Z_m, \oplus_m, \otimes_m$>为整环，故一定是域，且是有限域。

[延伸] 我们知道常见域如有理数域、实数域以及复数域的作用。例如，实系数代数方程在实数域内不一定可解，但实或复系数代数方程在复数域内均可解，从而不再需要更大的数域。含有有限个元素的有限域一般称为伽洛瓦域，它们在解方程、组合设计、纠错码、密码和信息安全等方面发挥着非常重要的作用[39,40]。

思考与练习 7.1

7-1　定义 **Z** 上的运算⊞和⊡如下：对 $\forall a,b \in \mathbf{Z}$，$a \boxplus b = a+b-1$，$a \boxdot b = a+b-a \cdot b$。证明<**Z**,⊞,⊡>是含幺交换环。

7-2　设<A,+,·>为环，且对 $\forall a \in A$，有 $a \cdot a = a$，则对 $\forall a \in A$，有 $a+a=0$，且 A 是交换环。

7-3　证明表 7-1 和表 7-2 定义的运算确定了一个整环<{0,1},⊞,⊡>。

表 7-1

⊞	0	1
0	0	1
1	1	0

表 7-2

⊡	0	1
0	0	0
1	0	1

7-4 设$<S,+,\cdot>$为代数系统，其中的运算$+$和$\cdot$为普通加法和乘法，S为下述集合：

(a) $S=\{x \mid x\geqslant 0, x\in \mathbf{Z}\}$。 (b) $S=\{2\cdot n \mid n\in \mathbf{Z}\}$。

(c) $S=\{2\cdot n+1 \mid n\in \mathbf{Z}\}$。 (d) $S=\{a/b \mid a,b\in \mathbf{Z}^{+}, a\neq k\cdot b, k\in \mathbf{Z}\}$。

(e) $S=\{a+b\sqrt{3} \mid a,b\in \mathbf{Q}\}$。 (f) $S=\{a+b\sqrt[4]{3} \mid a,b\in \mathbf{Q}\}$。

问$<S,+,\cdot>$是否为整环？是否为域？说明你的理由。

7-5 设$<A,+,\cdot>$为域。若$S\subseteq A$，$T\subseteq A$，且$<S,+,\cdot>$和$<T,+,\cdot>$都是域，证明$<S\bigcap T,+,\cdot>$也是域。

7-6 设$<A,+,\cdot>$为域。对$\forall a\in A$且$a\neq 0$，证明方程$a\cdot x+b=0$唯一可解。

7.2 格

格与布尔代数是一类从偏序关系衍生出来的特殊代数系统，在近代解析几何、开关理论和密码学等方面有很多直接应用。

7.2.1 格与其诱导的代数系统

[定义 7-5] 设$<L,\preccurlyeq>$是一个偏序集，如果对$\forall x,y\in L$，集合$\{x,y\}$存在上确界（最小上界，记作$\sup\{x,y\}$）和下确界（最大下界，记作$\inf\{x,y\}$），则称$<L,\preccurlyeq>$是**格**（lattice）。

在一般的偏序关系中，两个元素组成的集合可能没有上界，即使存在上界，也不一定有上确界。下确界也类似。

例如，图 7-1 所示的偏序关系中，子集$\{a,b\}$没有上界，a与b都是子集$\{c,d\}$的上界，但$\{c,d\}$没有最小上界。同时，子集$\{c,d\}$没有下界，尽管元素c和d都是子集$\{a,b\}$的下界，但子集$\{a,b\}$没有最大下界。

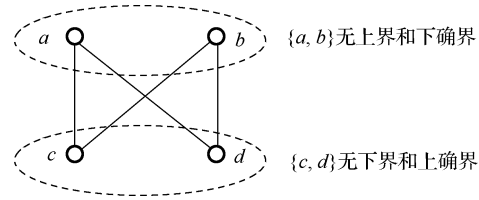


图 7-1

例 7-4 证明$<\mathbf{Z},\leqslant>$、集合S的幂集$\mathscr{P}(S)$与其上的包含关系$\subseteq$组成的偏序集$<\mathscr{P}(S),\subseteq>$都是格。

证明 在偏序集$<\mathbf{Z},\leqslant>$中，对$\forall x,y\in \mathbf{Z}$，有

$$\sup\{x,y\}=\max(x,y),\quad \inf\{x,y\}=\min(x,y)。$$

故$<\mathbf{Z},\leqslant>$是格。

在偏序集$<\mathscr{P}(S),\subseteq>$中，对任意的集合$A$和$B$，有

$$\sup\{A,B\}=A\bigcup B,\quad \inf\{A,B\}=A\bigcap B。$$

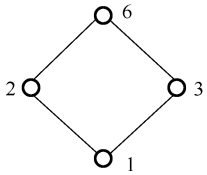
因此，$<\mathscr{P}(S),\subseteq>$是格。

例 7-5 对任意正整数n，若A_n表示n的正因子集合，说明$<A_n,|>$是格并绘制其哈斯图。

解 对$\forall x,y\in A_n$，有

$$\sup\{x,y\}=\mathrm{LCM}(x,y),\quad \inf\{x,y\}=\mathrm{GCD}(x,y)。$$

因此，$<A_n,|>$是格。这里的 GCD、LCM 分别是最大公约数和最小公倍数。



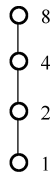


图 7-2

图 7-2 为 $n=6$ 和 $n=8$ 时的格$<A_6, |>$和$<A_8, |>$的哈斯图。

很明显，如果将上述讨论中的 A_n 换成 $\mathbf{Z}^+$即可说明$<\mathbf{Z}^+, |>$是格。

[辨析] 为什么称为“格”？那是因为在哈斯图中，任意 2 个元素加上其上确界和下确界体现出来的图形有“格子”的味道。

[定义 7-6] 设$<L,\leqslant>$是格，定义 L 上的两个运算 $\vee$ 和 $\wedge$（也可记作⊕和⊗、+和×等）。对 $\forall x,y\in L$，有

$$x\vee y=\sup\{x,y\},\quad x\wedge y=\inf\{x,y\}。$$

则称$<L,\vee,\wedge>$为格$<L,\leqslant>$所**诱导的代数系统**，并称 $\vee$ 和 $\wedge$ 为**并运算**和**交运算**。

为了叙述简单，可以直接称$<L,\vee,\wedge>$或者 L 为格，其含义都是指 $\vee$ 和 $\wedge$ 是在格$<L,\leqslant>$上依据上述定义产生的运算。

[定义 7-7] 设 P 是一个关于格的命题，若$\leqslant$与$\geqslant$互换，将 $\vee$ 与 $\wedge$ 互换，得到的新命题 P^*称为 P 的**对偶命题**。这里的 $b\geqslant a$ 是指 $a\leqslant b$。

[定理 7-3] 若 P 是一个关于任意格都为真的命题，则其对偶命题 P^*也是真命题。

证明　略。此定理称为**格的对偶原理**。

例如，对任意格都有 $a\leqslant a\vee b$，因此，必有 $a\geqslant a\wedge b$，即 $a\wedge b\leqslant a$。因此，在研究格的性质时，一般可以仅讨论对偶命题中的一个命题的真伪。

[定理 7-4] 若$<L,\vee,\wedge>$为格，则

(1) 对 $\forall a,b\in L$，$a\leqslant a\vee b$ 且 $b\leqslant a\vee b$。

(2) 对 $\forall a,b,c,d\in L$，若 $a\leqslant b$ 且 $c\leqslant d$，必有 $a\vee c\leqslant b\vee d$。

证明　(1) 由运算定义是显然的。

(2) 因为 $b\vee d$ 是 b 和 d 的上界，由传递性，也是 a 和 c 的上界，而 $a\vee c$ 是 a 和 c 的最小上界，故结论成立。

格所诱导的代数系统满足大多数算律。

[定理 7-5] 若$<L,\vee,\wedge>$为格，则 $\vee$ 和 $\wedge$ 运算满足交换律、结合律、幂等律和吸收律，即对 $\forall a,b,c\in L$，有

(1) $a\vee b=b\vee a$，$a\wedge b=b\wedge a$（交换律）。

(2) $a\vee(b\vee c)=(a\vee b)\vee c$，$a\wedge(b\wedge c)=(a\wedge b)\wedge c$（结合律）。

(3) $a\vee a=a$，$a\wedge a=a$（幂等律）。

(4) $a\vee(a\wedge b)=a$，$a\wedge(a\vee b)=a$（吸收律）。

证明　仅证(2)和(4)。

(2) 因为

$$b\leqslant b\vee c\leqslant a\vee(b\vee c),\quad a\leqslant a\vee(b\vee c)。$$

有

$$a \vee b \preccurlyeq a \vee (b \vee c)。$$

又因为 $c \preccurlyeq b \vee c \preccurlyeq a \vee (b \vee c)$，故

$$(a \vee b) \vee c \preccurlyeq a \vee (b \vee c)。$$

类似地，可证明 $a \vee (b \vee c) \preccurlyeq (a \vee b) \vee c$。

由反对称性得 $a \vee (b \vee c) = (a \vee b) \vee c$。利用对偶原理可得 $a \wedge (b \wedge c) = (a \wedge b) \wedge c$。

(4) 显然，$a \preccurlyeq a \vee (a \wedge b)$。因为 $a \preccurlyeq a$，且 $a \wedge b \preccurlyeq a$，故

$$a \vee (a \wedge b) \preccurlyeq a。$$

由反对称性得 $a \vee (a \wedge b) = a$。利用对偶原理可得 $a \wedge (a \vee b) = a$。

[辨析] 格中等式的证明主要依赖反对称性。

事实上，如果一个代数系统<$L, \vee, \wedge$>的两个二元运算 $\vee$ 和 $\wedge$ 满足交换律、结合律和吸收律，也能够确定一个对应的偏序关系 $\preccurlyeq$，使<$L, \preccurlyeq$>是格。

7.2.2 子格

[定义 7-8] 设<$L, \preccurlyeq$>为格，S 为 L 的非空子集。若 S 对格诱导的运算 $\vee$ 和 $\wedge$ 封闭，则称<$S, \preccurlyeq$>为<$L, \preccurlyeq$>的**子格**。

例如，<$\mathbf{Z}^+, |$>是格。记 E^+为所有正偶数集合，显然，E^+对运算 $\vee$ 和 $\wedge$ 是封闭的，故<$E^+, |$>是<$\mathbf{Z}^+, |$>的子格。

可以证明，子格一定是格。但是，对于任意的非空子集 $S \subseteq L$，<$S, \preccurlyeq$>不一定是格，且即使是格，也不一定是子格。

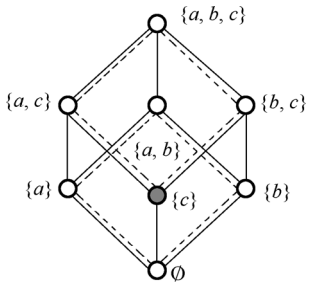


图 7-3

例如，设 $S=\{a,b,c\}$，格<$\mathscr{P}(S), \subseteq$>的哈斯图如图 7-3 所示。其中，<$\{\{c\},\{a,c\},\{b,c\},\{a,b,c\}\}, \subseteq$>、<$\{\varnothing,\{a\},\{b\},\{a,b\}\}, \subseteq$>是子格。<$\mathscr{P}(S)-\{\{c\}\}, \subseteq$>虽然是格，但不是子格，因为 $\{a,c\} \wedge \{b,c\} = \{c\} \notin \mathscr{P}(S)-\{\{c\}\}$，运算对子集 $\mathscr{P}(S)-\{\{c\}\}$ 不封闭。

例 7-6 设<$L, \preccurlyeq$>是格，任取 $a \in L$，定义 L 的子集 S 为

$$S = \{x \mid x \in L \text{且} x \preccurlyeq a\}。$$

则<$S, \preccurlyeq$>是<$L, \preccurlyeq$>的子格。

证明 对 $\forall x, y \in S$，因为 $x \preccurlyeq a$，$y \preccurlyeq a$，即 a 是 x 和 y 的上界，故 $x \vee y \preccurlyeq a$，$x \wedge y \preccurlyeq a$，即 S 对运算封闭。结论成立。

7.2.3 特殊格

1. 分配格

[定义 7-9] 设<$L, \vee, \wedge$>为格，如果运算 $\vee$ 和 $\wedge$ 满足分配律，即对 $\forall a,b,c \in L$，有

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c),\ a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)。$$

则称<$L, \preccurlyeq$>为**分配格**。

例 7-7　说明图 7-4 中的哪些格是分配格。

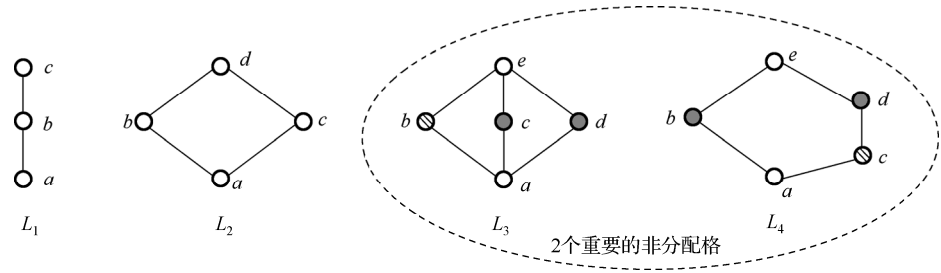


图 7-4

解　L_1 和 L_2 是分配格，L_3 和 L_4 不是分配格。在 L_3 中，有

$$b \wedge (c \vee d) = b \wedge e = b, (b \wedge c) \vee (b \wedge d) = a \vee a = a。$$

在 L_4 中，有

$$c \vee (b \wedge d) = c \vee a = c, (c \vee b) \wedge (c \vee d) = e \wedge d = d。$$

格 L_3 和 L_4 分别称为“钻石格”和“五角格”，它们在分配格的判别中有重要作用。

[定理 7-6] 若 L 是格，则 L 是分配格当且仅当 L 不含有与钻石格和五角格同构的子格。

证明　略。

这里的同构是指几个元素的名字、左右位置等可以不同，但元素间的大小关系是一致的。

例如，图 7-5 中的格都不是分配格，A_1 含有与钻石格同构的子格，A_2 和 A_3 含有与五角格同构的子格。

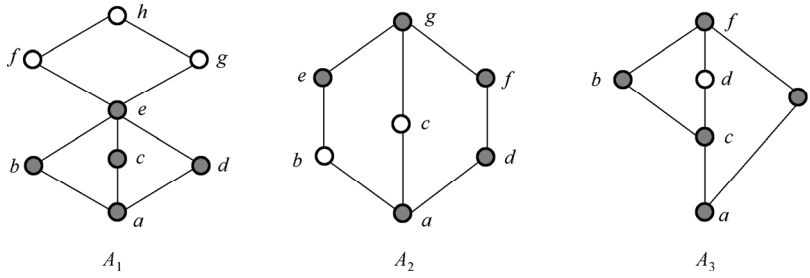


图 7-5

[辨析] 在利用此定理进行判别时，重要的问题是“子格”的概念。例如，对于格 A_3，尽管 $S=\{f, b, d, e, a\}$ 与钻石格 L_3 同构，不能由此判定 A_3 不是分配格。这是因为 $b \wedge d = c$，但 $c \notin S$，运算 $\wedge$ 对 S 不封闭。可见 S 仅为 A_3 的一个普通子集而非子格。

[定理 7-7] 链是分配格。

证明　设$<L,\leqslant>$是链，则$<L,\leqslant>$显然是格。对 $\forall a,b,c \in L$，可能有如下关系：

(1) a 最大，即 $b \leqslant a$ 且 $c \leqslant a$。有

$$b \vee c \leqslant a,\ a \wedge (b \vee c) = b \vee c = (a \wedge b) \vee (a \wedge c)。$$

(2) a 非最大，即 $a \leqslant b$ 或 $a \leqslant c$，不妨设 $a \leqslant b$。因为 $b \leqslant b \vee c$，有

$$a \wedge (b \vee c) = a。$$

因 $a \wedge b = a$，$a \wedge c \leqslant a$，有

$$(a \wedge b) \vee (a \wedge c) = a。$$

即 $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$。

2．有界格

[定义 7-10] 设<L,$\leqslant$>是格，若 $\exists a \in L$，使得 $\forall x \in L$，$a \leqslant x$，称 a 为 L 的**全下界**。若 $\exists b \in L$，使得 $\forall x \in L$，$x \leqslant b$，称 b 为 L 的**全上界**。

例如，在图 7-5 中，a 和 h 分别是格 A_1 的全下界和全上界。

由反对称性很容易说明，若格的全下（上）界存在则必唯一。

[定义 7-11] 设<L,$\leqslant$>是格，且存在全上界和全下界，则称 L 为**有界格**。通常，格的全下界和全上界分别记作 0 和 1，并将有界格所诱导的代数系统记作<L,$\vee$,$\wedge$,0,1>。

例如，对任意集合 S，<$\mathscr{P}(S)$,$\subseteq$>为有界格，$\varnothing$ 和 S 分别为全下界和全上界。偏序集<{x|$x \in \mathbf{R}$且$0 \leqslant x \leqslant 1$},$\leqslant$>也是有界格，0 和 1 是它的全下界和全上界。

任意有限格 $L = \{a_1, a_2, \cdots, a_n\}$ 显然是有界格，因为 $a_1 \wedge a_2 \wedge \cdots \wedge a_n$ 和 $a_1 \vee a_2 \vee \cdots \vee a_n$ 分别为全下界和全上界。

有界格的重要性质是其诱导的代数系统满足同一律和零律。

[定理 7-8] 设<L,$\vee$,$\wedge$,0,1>为有界格，对 $\forall a \in L$，有

(1) $a \vee 0 = a$，$a \wedge 1 = a$（同一律）。

(2) $a \vee 1 = 1$，$a \wedge 0 = 0$（零律）。

证明 因 0 是全下界，$0 \leqslant a$，且 $a \leqslant a$，有

$$a \vee 0 \leqslant a。$$

因为 $a \vee 0$ 为 a 和 0 的上界，有

$$a \leqslant a \vee 0。$$

得 $a \vee 0 = a$。其他等式的证明类似。

3．有补格

[定义 7-12] 设<L,$\vee$,$\wedge$,0,1>为有界格，对 $\forall a \in L$，若 $\exists b \in L$，使得

$$a \wedge b = 0,\ a \vee b = 1。$$

则称 b 为 a 的**补元**，记作 $\overline{a}$。当然，a 也是 b 的补元，即补元是相互的。

例如，对图 7-4 中的格 L_1，a 和 c 分别为 0 和 1，且互为补元，b 没有补元；对五角格 L_4，a 和 e 分别为 0 和 1，且互为补元，b 的补元为 c 和 d，c 和 d 的补元都是 b。

[辨析] *在有界格中，0 和 1 总是互为补元。*

[定理 7-9] 设<$L,\vee,\wedge,0,1$>为有界分配格。若 $a\in L$ 存在补元，则补元是唯一的。

证明　若 b 和 c 都是 a 的补元，则

$$a\wedge b=a\wedge c=0,\quad a\vee b=a\vee c=1。$$

因此，有

$$(a\wedge b)\vee c=0\vee c=c\ 。$$

因为 L 是分配格，且格满足交换律和吸收律，有

$$\begin{aligned}(a\wedge b)\vee c&=(a\vee c)\wedge(b\vee c)=(a\vee b)\wedge(b\vee c)\\&=b\vee(a\wedge c)=b\vee(a\wedge b)=b\vee 0=b。\end{aligned}$$

故 $b=c$。

[定义 7-13] 设<$L,\preccurlyeq$>为有界格，若 L 的所有元素都存在补元，则称 L 为**有补格**。

例如，图 7-4 中的 L_2、L_3 和 L_4 都是有补格，但 L_1 不是有补格。

在一个有补格<$L,\preccurlyeq$>中，因为每个元素都有补元，因此，对 $\forall a\in L$，$\exists\overline{a}\in L$，使得

$$a\wedge\overline{a}=0,\quad a\vee\overline{a}=1。$$

此算律称为**互补律**或**补元律**。

思考与练习 7.2

7-7　有补格一定是有界的吗？补元是唯一的吗？什么条件能够保证补元是唯一的？

7-8　说明图 7-6 的偏序集中哪些是格，哪些是分配格。

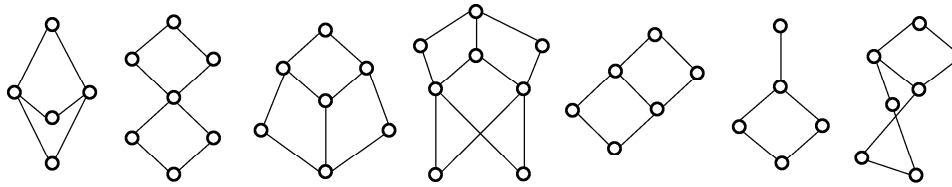


图 7-6

7-9　设$\preccurlyeq$为集合 L 上的整除关系，说明其中哪些系统<$L,\preccurlyeq$>是格。

(a) $L=\{1,2,3,4,6,12\}$；　　(b) $L=\{1,2,3,4,6,8,12,14\}$；

(c) $L=\{n\mid 1\preccurlyeq n\preccurlyeq 12,n\in\mathbf{Z}\}$。

7-10　设$<L,\preccurlyeq>$是格，任取 $a,b\in L$，$a\prec b$，构造集合 $B=\{x\mid x\in L,a\preccurlyeq x\preccurlyeq b\}$。证明$<B,\preccurlyeq>$是格。

7-11　证明：在格中，若 $a\preccurlyeq b\preccurlyeq c$，则

(a) $a\vee b=b\wedge c$。　　(b) $(a\wedge b)\vee(b\wedge c)=(a\vee b)\wedge(b\vee c)=b$。

7-12 举出 2 个含有 6 个元素的格，其中一个是分配格，另一个不是分配格。

7-13 在图 7-7 所示的有界格中回答：

(a) a 和 f 的补元是什么？ (b)它是分配格吗？

(c) 它是有补格吗？

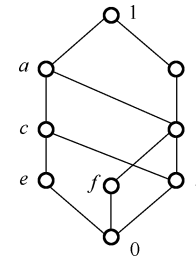


图 7-7

7-14 证明<**Z**,max,min>是分配格。

7-15 证明在元素个数大于 1 的格中，不存在以自身为补元的元素。

7-16 证明钻石格和五角格是有补格。

7-17 证明具有 3 个及更多元素的链不是有补格。

7.3 布 尔 代 数

7.3.1 布尔格诱导的布尔代数

[定义 7-14] 一个有补分配格称为**布尔格**。在有补分配格<B,$\preccurlyeq$>中，将“求补”定义为一元运算$'$：对 $\forall a \in B$，有

$$a' = \overline{a}。$$

其中的 $\overline{a}$ 为 a 的补元（也可以直接用“$^-$”表示求补运算）。称<$B,\vee,\wedge,',0,1$>为由布尔格<B,$\preccurlyeq$>诱导的**布尔代数**（Boolean algebra），在 B 为有限集时称为**有限布尔代数**。

例如，对任意的非空集合 S，<$\mathscr{P}(S),\subseteq$>是布尔格。这是因为集合的交、并运算满足分配律，$\varnothing$ 和 S 分别为全下界 0 和全上界 1。对 $\forall X \in \mathscr{P}(S)$，$S - X$ 为其补元。<$\mathscr{P}(S),\subseteq$>诱导的布尔代数就是<$\mathscr{P}(S),\cup,\cap,\sim,\varnothing,S$>。

几种特殊格之间的关系及其应满足的算律可由图 7-8 反映出来。

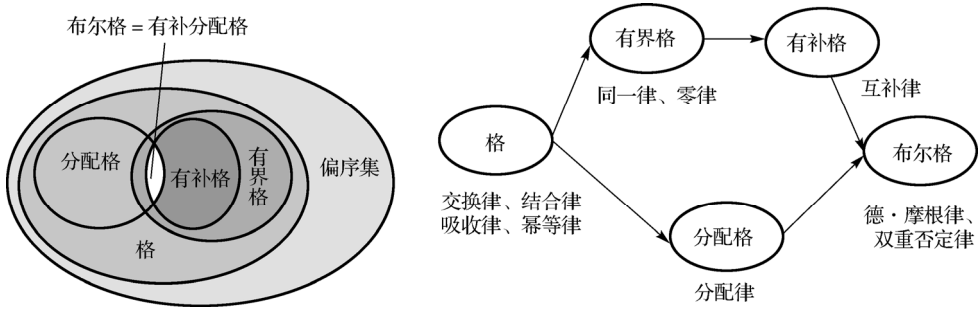


图 7-8 格之间的关系及其满足的算律

[定理 7-10] 若 $<B,\vee,\wedge,',0,1>$ 为布尔代数，则

(1) $\forall a \in B$，有 $(a')' = a$（双重否定律）。

(2) $\forall a,b \in B$，$(a \wedge b)' = a' \vee b'$，$(a \vee b)' = a' \wedge b'$（德·摩根律）。

证明

(1) 因为 $(a')'$ 和 a 都是 a' 的补元，由补元的唯一性，得 $(a')'=a$。

(2) 因为

$$(a\wedge b)\vee(a'\vee b')=(a\vee a'\vee b')\wedge(b\vee a'\vee b')=1\wedge 1=1,$$

$$(a\wedge b)\wedge(a'\vee b')=(a\wedge b\wedge a')\vee(a\wedge b\wedge b')=0\vee 0=0。$$

因此，有 $(a\wedge b)'=a'\vee b'$。同理，$(a\vee b)'=a'\wedge b'$。

注意到当 $|S|=n$ 时，有 $|\mathscr{P}(S)|=2^n$。实际上，这是一个一般的现象。可以证明：对任意的正整数 n，必存在含有 2^n 个元素的布尔代数；反之，任一个有限布尔代数的元素个数必为 2^n，且元素个数相同的布尔代数都是同构的。

7.3.2　典型的布尔代数

布尔代数是由英国数学家乔治·布尔（George Boolean）于 1849 年创立的。与一般的代数系统不同，布尔代数描述的是客观事物之间的逻辑关系而非数量关系，其核心在于建立在集合上的一些算律。总体上，布尔代数具有 10 个性质（算律），参见图 7-8，其中最基本的算律包括交换律、分配律、同一律和互补律。因此，可以直接将其以如下方式定义出来：

[定义 7-15] 若 $<B,\vee,\wedge,\bar{},0,1>$ 是一个代数系统，其运算满足交换律、分配律、同一律和互补律，则称 $<B,\vee,\wedge,\bar{},0,1>$ 为**布尔代数**。

上述定义被称为布尔代数的公理化定义。可以证明，它与布尔代数的格定义是等价的。布尔代数中的三种运算通常被称为 NOT（非，补运算）、AND（与，布尔积）和 OR（或，布尔和）。

应用最为广泛的典型布尔代数是二值布尔代数，即令 B={0,1}。布尔代数 $<B,\vee,\wedge,\bar{},0,1>$ 提供了{0, 1}集合上的如下运算规则：

(1) 补运算：$\overline{0}=1$，$\overline{1}=0$。

(2) 布尔和：0∨0=0，0∨1=1，1∨0=1，1∨1=1。

(3) 布尔积：0∧0=0，0∧1=0，1∧0=0，1∧1=1。

符号 $\vee$ 和 $\wedge$ 可用+和·代替。利用这些规则，复杂的逻辑问题可以被转换为简单的符号演算。同时，结合布尔代数所具有的性质，一个复杂的逻辑电路也可以被有效地简化。

在逻辑（数字）电路设计中，基本问题是依据一组输入和输出确定对应的电路。如果一组自变量 $x_1,x_2,\cdots,x_n$ 代表着一组开关量输入，电路对应着从 $\{0,1\}^n$ 到 $\{0,1\}$ 的函数 f，那么，函数 f 的结果对应着 2^n 种可能的输入，每种输入有 2 种可能的输出，可用列表法来描述。表 7-3 给出了一个从 $\{0,1\}^2$ 到 $\{0,1\}$ 的函数示例。

表 7-3　函数 *f* 的描述

输入	输出
<0, 0>	0
<0, 1>	1
<1, 0>	1
<1, 1>	0

无论是问题分析或电路设计，这种表示方法都因过于麻烦而难以接受，需要采用布尔表达式来简化。

[定义 7-16] 设 $<B=\{0,1\},\vee,\wedge,\bar{},0,1>$ 为布尔代数，定义**布尔表达式**如下：

(1) B 中的任何元素（常量）或用于表示它们的变元是布尔表达式；

(2) 如果 e_1 和 e_2 是布尔表达式，则 $\overline{e_1}$、$e_1 \vee e_2$ 和 $e_1 \wedge e_2$ 是布尔表达式；

(3) 只有有限次运用规则(2)构造出的符号串是布尔表达式。

含有 n 个变元的布尔表达式称为 ***n* 元布尔表达式**，记作 $E(x_1, x_2, \cdots, x_n)$。

例如，$0 \wedge x_1$、$(1 \vee \overline{x_1}) \wedge x_2$、$((x_1 \vee \overline{x_2}) \wedge \overline{0}) \vee \overline{(x_1 \wedge x_3)}$ 分别是一元、二元和三元布尔表达式。

很明显，$B=\{0, 1\}$上的 n 元布尔表达式都是 $B^n = \{< x_1, x_2, \cdots, x_n > | \, x_i \in B, 1 \leqslant i \leqslant n\}$ 到 B 的函数，称为“n 元布尔函数”，它与一般的数学函数十分相近，但自变量和函数的取值仅限于 B。例如，以下为布尔代数 $< B = \{0,1\}, \vee, \wedge, \overline{\ }, 0, 1 >$ 上的一个三元布尔表达式：

$$E(x_1, x_2, x_3) = (x_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{x_2}) \wedge \overline{(x_2 \vee x_3)}。$$

如果变元（自变量）的一组赋值为 x_1=1，x_2=0，x_3=1，则可依据运算律求得表达式的值：

$$E(1,0,1) = (1 \vee 0) \wedge (\overline{1} \vee \overline{0}) \wedge \overline{(0 \vee 1)} = 1 \wedge 1 \wedge 0 = 0。$$

对于一般的 n 和布尔代数 B，并非所有从 B^n 到 B 的函数都可以采用布尔表达式来表示，但可以证明，对于 $n=2$ 的特殊情形，$\{0, 1\}^n$ 到$\{0, 1\}$的函数与$\{0, 1\}$上的布尔表达式是同义的。

[定理 7-11] 对于两个元素的布尔代数$<B=\{0, 1\}, \vee, \wedge, \overline{\ }, 0, 1>$，任何一个从$\{0, 1\}^n$ 到$\{0, 1\}$的函数都是布尔表达式。

定理说明，在二值逻辑中，具有任何输入、输出关系的电路都可以采用布尔表达式来描述。这是数字电路设计的理论基础。

不过，从实际的逻辑问题中概括出来的逻辑函数不一定是最简的，利用规则对布尔表达式进行化简可以简化电路设计，减少使用的基本电路（称为“门电路”）数量，降低系统成本，还可以提高系统的可靠性。

例如，有如下布尔函数：

$$E(x_1, x_2, x_3) = (x_1 \wedge x_2 \wedge \overline{x_3}) \vee (x_1 \wedge \overline{x_2} \wedge x_3) \vee (\overline{x_1} \wedge x_2) \vee x_2 \vee (x_2 \wedge x_3)。$$

直接由函数组成电路时需要采用图 7-9 所示的电路图。但经过等价化简后，其函数表达式为

$$E(x_1, x_2, x_3) = (x_1 \wedge x_3) \vee x_2。$$

于是，可以将其简化为图 7-10 所示的电路图。

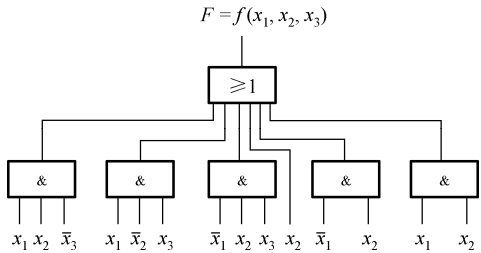


图 7-9

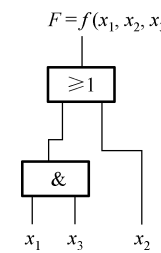


图 7-10

简化布尔表达式需要遵循一定的原则，也存在一些有效的方法，如卡诺图等，这些内容可以在数字逻辑书籍中了解。

布尔代数的广泛应用源自计算机领域大量存在的二值问题。例如，命题逻辑可以用布尔代数$<\{\mathbf{F},\mathbf{T}\},\vee,\wedge,'>$来描述，开关代数可以用<{断开,闭合},并联,串联,反向>来描述，它们都是布尔代数$<\{0,1\},\vee,\wedge,\overline{\ }>$的具体表现，具有相同的运算规律。

[延伸] 布尔代数的应用范围十分广泛，最明显的应用就是形式逻辑推理和电路理论设计。当然，即便在程序设计语言中，布尔代数也随处可见。例如，C 语言中的位运算就是布尔运算，如果一个对象具有 4 种属性，用 1111 的每一位代表一种属性，利用 1111&1110 就可以去掉最后一种属性[41, 42]。

思考与练习 7.3

7-18　布尔代数主要满足哪些算律？核心算律是什么？

7-19　证明在布尔代数中，有

(a) $a\vee(a'\wedge b)=a\vee b$。　　(b) $a\wedge(a'\vee b)=a\wedge b$。

7-20　在布尔代数$<B,\vee,\wedge,'>$中定义运算⊞和⊡为：

$$a\boxplus b=(a\wedge b')\vee(a'\wedge b),\ a\boxdot b=a\wedge b。$$

证明$<B,\boxplus,\boxdot>$是环。

7-21　验证上题中的运算满足：

(a) $(a\boxplus b)\boxplus b=a$。　　(b) $a\boxplus 1=a'$。

7-22　设 $A=\{1,2,3,4,6,12\}$、$B=\{1,2,3,4,6,8,12,24\}$ 和 $C=\{1,2,5,10,11,22,55,110\}$，说明<$A$,LCM, GCD,′>、<$B$,LCM,GCD,′>和<$C$,LCM,GCD,′>是否为布尔代数。

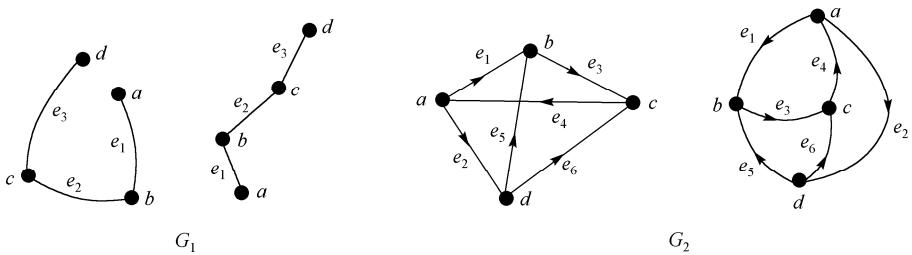
第 8 章　图

图作为一种工具，能提供对问题和已知信息的一种清晰和直观的表达，正如采用关系图来表示关系时所看到的那样。一般认为，图论（graph theory）作为数学的一个分支，起源于欧拉对著名的哥尼斯堡七桥问题的研究，但它的应用几乎遍布于科学研究与生产实践的每个领域。

8.1　图的基本概念

简单地说，图是由结点和结点之间的连线组成的图形，线长及结点位置无关紧要。例如，图 8-1 中的两组图中的两个图都各自相同。

[辨析] 图论关心的是图形的拓扑结构，即研究与大小、形状无关的点和线之间的关系。



G_1　　G_2

图 8-1

8.1.1　图的认知

[定义 8-1] 一个图 G 是一个序偶（二元组）$<V,E>$或$<V(G),E(G)>$，其中的 $V=\{v_1,v_2,\cdots,v_n\}$ 是一个非空的**结点**（vertex，或称**顶点**）集合，$E=\{e_1,e_2,\cdots,e_m\}$ 是图的**边**（edge）集合。如果所有边没有方向（称为**无向边**），称 G 为**无向图**（undigraph）。如果所有边含有方向（称为**有向边**或**弧**），称 G 为**有向图**（digraph）。图的结点数称为图的**阶数**。

图 8-1 中的 G_1 和 G_2 分别是无向图和有向图。几个城市用高速公路连接起来的交通图通常是无向图。计算机网络一般是一个有向图，因为在网络图中，一些连接可以只对一个方向操作，如将数据传到数据中心。

通常，边用与其连接的两个结点来表示。为了区分无向边和有向边，分别采取“(a,b)”和“$<a,b>$”来说明其是否包含方向。可见，对于无向图，边集 E 是结点 V 中元素组成的无序对集合，而有向图的边集 E 是结点 V 中元素组成的有序对（序偶）集合，即 E 是 $V\times V$ 的子集。有向边用箭头表示方向，还可称其为“弧”。

例如，对于图 8-1 中的无向图和有向图，分别表示为：

G_1：$V(G_1)=\{a,b,c,d\}$，$E(G_1)=\{(a,b),(b,c),(c,d)\}$，

G_2：$V(G_2)=\{a,b,c,d\}$，$E(G_2)=\{<a,b>,<a,d>,<b,c>,<c,a>,<d,b>,<d,c>\}$。

为了简单，通常直接用点对描述边而不标记边名 e_i。

[辨析] 对于有向边<*a*,*b*>，箭头指向 *b*。

在理解图时需要了解一些基本概念和名词。

[定义 8-2] 在一个图中：

(1) 边 *e* 与其组成顶点 *a* 和 *b* 之间称为**关联**（incident）。其中，*a* 和 *b* 是 *e* 关联的结点，*e* 是与 *a* 和 *b*（或(*a*,*b*)，或<*a*,*b*>）相关联的边。

(2) 在有向边<*a*,*b*>中，*a* 称为边的**起始结点**，*b* 称为边的**终止结点**。

(3) 若两个结点 *a* 和 *b* 由一条有向边（或无向边）关联，则称 *a* 与 *b* 是**邻接点**；关联于同一结点 *a* 的两条边 e_1 和 e_2 称为**邻接边**或**相邻边**。

(4) 不与任何结点相邻接的结点称为**孤立结点**。

(5) 关联于同一结点的一条边称为**自回路**或**环**。环的方向是没有意义的，它既可作为有向边也可作为无向边。如图 8-2 中 G_1 的 e_6 和 G_2 的 e_7。

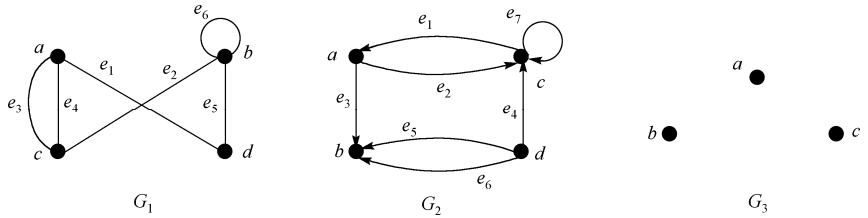


图 8-2

(6) 关联于同一对结点的方向相同的边称为**重复边**或**平行边**。例如，图 8-2 中 G_1 的 e_3 与 e_4 和 G_2 的 e_5 与 e_6。不过，G_2 的 e_1 与 e_2 不是平行边，因为二者的方向不同。

(7) 仅由孤立结点组成的图称为**零图**。或者说，零图是边集为空集的图，如图 8-2 中的 G_3。

(8) 仅由一个孤立结点构成的图称为**平凡图**。

(9) 含有平行边的图称为**多重图**。如图 8-2 中的 G_1 与 G_2 都是多重图。

(10) 不含平行边和环的图称作**简单图**。如图 8-1 中的 G_1 与 G_2 都是简单图。

在复杂的图中，还可能同时存在无向边和有向边，称为“混合图”。

8.1.2　结点的度与握手定理

1．结点的度

[定义 8-3] 一个图 $G=<V,E>$中，与结点 $v\in V$ 关联的边数称作该结点的**度**（**数**）（degree），记作 $d_G(v)$，或简记为 $d(v)$。对于有向图，结点的度被更细致地分为入度和出度。对于结点 $v\in V$，射出 *v* 的边数称为 *v* 的**出度**，记作 $d^+(v)$，射入 *v* 的边数称为 *v* 的**入度**，记作 $d^-(v)$。

[辨析] 也可以用 $\mathrm{d}^+(v)$ 表示入度，用 $\mathrm{d}^-(v)$ 作为出度。

[辨析] 结点 v 的度也可记作 $\deg(v)$，但本书用 $\deg(r)$表示平面图中面的次数。

显然，对于任意结点 v，$\mathrm{d}(v)=\mathrm{d}^+(v)+\mathrm{d}^-(v)$，即结点的出度与入度之和等于该结点的度。

因为环意味着两条边，故每个环为其对应结点上的度数增加 2。

例如，对于图 8-2 中的 G_2，$\mathrm{d}(c)=5$，$\mathrm{d}^+(c)=2$，$\mathrm{d}^-(c)=3$。

[定义 8-4] 若 G 为无向图，称 $\Delta(G)=\max\limits_{v\in V}\{\mathrm{d}(v)\}$ 为图 G 的**最大度**，称 $\delta(G)=\min\limits_{v\in V}\{\mathrm{d}(v)\}$ 为图 G 的**最小度**。在有向图 G 中可以按出度和入度单独计算，分别称 $\Delta^+(G)=\max\limits_{v\in V}\{\mathrm{d}^+(v)\}$、$\delta^+(G)=\min\limits_{v\in V}\{\mathrm{d}^+(v)\}$ 为**最大出度**和**最小出度**，称 $\Delta^-(G)=\max\limits_{v\in V}\{\mathrm{d}^-(v)\}$、$\delta^-(G)=\min\limits_{v\in V}\{\mathrm{d}^-(v)\}$ 为**最大入度**和**最小入度**。

例如，对于图 8-2 中的 G_1，$\Delta(G_2)=4$，$\delta(G_2)=2$。

2．握手定理

[定理 8-1] 对任意的图 $G=<V,E>$，结点度数的总和等于边数的两倍，即

$$\sum_{v\in V}\mathrm{d}(v)=2|E|。$$

此定理被称为“**握手定理**”。

证明 因为每条边必关联两个结点，而一条边给予关联的每个结点的度数为 1。因此，一个图中的结点度数总和等于边数的两倍。

例 8-1 任何图中度数为奇数的结点个数必是偶数。

证明 很明显，所有度数为偶数的结点的总度数为偶数，为了满足握手定理，要保证奇数度结点的度数之和也是偶数。因此，就必须包含偶数个奇数度的结点。

[定理 8-2] 在有向图 $G=<V,E>$中，所有结点的入度之和等于所有结点的出度之和，即

$$\sum_{v\in V}\mathrm{d}^+(v)=\sum_{v\in V}\mathrm{d}^-(v)=|E|。$$

证明 因为每一条有向边必对应一个入度和一个出度，若一个结点具有一个入度或出度，则必关联一条有向边，所以，有向图中各结点入度之和等于边数$|E|$，各结点出度之和也等于边数$|E|$，二者相等。

例 8-2 在一个图 $G=<V,E>$中，$|E|=|V|+1$，证明 G 中存在结点 v 满足 $\mathrm{d}(v)\geqslant 3$。

证明 若对 $\forall v\in V$，$\mathrm{d}(v)\leqslant 2$，则

$$\sum_{v\in V}\mathrm{d}(v)\leqslant 2|V|=2(|E|-1)\neq 2|E|。$$

与握手定理矛盾，故必 $\exists v\in V$，使 $\mathrm{d}(v)\geqslant 3$。

3．结点的度序列

一个图中对所有结点的度有什么要求呢？

在一个图 $G=<V=\{v_1,v_2,\cdots,v_n\},E>$中，数列 $\mathrm{d}(v_1),\mathrm{d}(v_2),\cdots,\mathrm{d}(v_n)$ 被称为 G 的**度序列**，甚至对有向图还可分为出度序列和入度序列。利用握手定理和出度与入度的关系，可以对结点的数量和性质进行粗略估计。

[定理 8-3] 非负整数序列 $d_1,d_2,\cdots,d_n$ 是某个图的度序列当且仅当 $\sum_{i=1}^{n}d_i$ 是偶数。

证明　由握手定理知必要性成立。

对于充分性，令 $d_1,d_2,\cdots,d_n$ 对应结点 $v_1,v_2,\cdots,v_n$。对任意的 d_i，若 d_i 为偶数，以 v_i 为结点做 $d_i/2$ 个环；若 d_i 为奇数，以 v_i 为结点做 $(d_i-1)/2$ 个环。因为有偶数个 d_i 为奇数，将其对应的结点两两配对并连线，就得到了对应的图。

上述证明给出了根据度序列构造对应图的一种方法，事实上，满足一个度序列的图通常会很多。一个非负整数序列 $d_1,d_2,\cdots,d_n$ 是某个图的度序列也称为该序列是“可图化”的。

例 8-3　说明以下两数列是否可以构成无向图的度序列：

(1) 2,3,4,5,6,7。　　(2) 1,2,2,3,4。

解　(1) 因为数列中奇数度的结点个数为 3，非偶数，不能构成度序列。

(2) 数列中有 2 个奇数度结点，可以构成度序列。图 8-3 为两个以其为度序列的图示例。

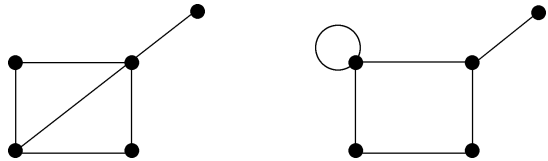


图 8-3

8.1.3　完全图与正则图

[定义 8-5] 对于简单图 $G=<V,E>$，若每对结点间都有边，则称该图为**完全图**（complete graph）。n 阶无向完全图记作 K_n。

图 8-4 显示了无向完全图 K_3 和 K_5，以及 3 阶有向完全图。

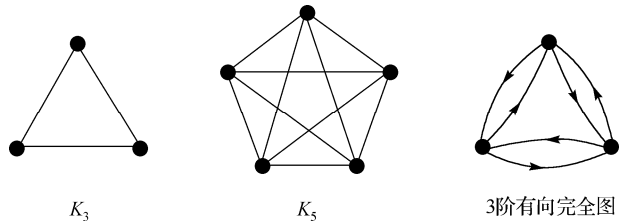


图 8-4

[定理 8-4] n 阶无向完全图 K_n 的边数为 $n(n-1)/2$。

证明　等同于 n 个结点中任取两点的组合数，故结论成立。

[定义 8-6] 对于简单图 $G=<V,E>$，若各结点度数相同，即 $\Delta(G)=\delta(G)=k$，则称该图为 ***k*-正则图**（regular graph）。

显然，完全图都是正则图。

由握手定理可知，n 阶 $k-$正则图的边数为 $kn/2$。

8.1.4 子图、补图与图同构

[定义 8-7] 设图 $G=<V,E>$，如果有图 $G'=<V',E'>$ 满足 $V'\subseteq V$，$E'\subseteq E$，则称 G' 是 G 的**子图**（subgraph），G 为 G' 的**母图**（supergraph）。若 $G'\subseteq G$ 且 $G'\neq G$，即 $V'\subset V$ 或 $E'\subset E$，则称 G' 是 G 的**真子图**。如果 $V'=V$，则称 G' 是 G 的**生成子图**或**支撑子图**（spanning subgraph）。

[辨析] “生成”意味着子图与母图结点相同，或者说子图包含了母图的所有结点。

例如，图 8-5 中的 G_1 为 K_5 的子图，而 G 和 $\overline{G}$ 为 K_5 的生成子图。它们都是真子图。

[定义 8-8] 设图 $G=<V,E>$ 是有 n 个结点的简单无向图，记 $K_n=<V,E_n>$，$\overline{E}=E_n-E$，则图 $\overline{G}=<V,\overline{E}>$ 称为 G 的**补图**（complementary graph）。

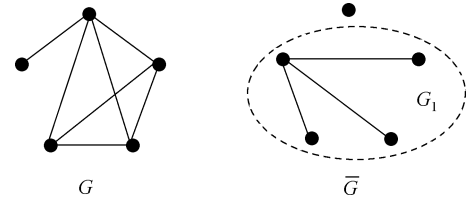


图 8-5

图 8-5 说明了一个图 G 及其补图 $\overline{G}$。由于补图是相对完全图定义的，在完全图中去掉某个图的边就得到其补图。因此，一个图与其补图是互补的。

[辨析] 补图存在着不同的定义：对图 $G=<V,E>$ 和其子图 $G_1=<V_1,E_1>$，若有图 $G_2=<V_2,E_2>$，$E_2=E-E_1$，V_2 是 E_2 的边所关联的结点集合，则 G_2 是 G_1 相对于 G 的补图，也称为广义补图。若 G 是无向完全图，则称 G_2 是 G_1 相对于完全图的补图，或 G_2 是 G_1 的（绝对）补图，记作 $\overline{G_1}$。在此定义下，一个图与其补图可能具有不同的结点集。因此，图与其补图不是互补的。

[定义 8-9] 对图 $G=<V,E>$ 和 $G'=<V',E'>$，若存在双射 φ：$V\to V'$，使得对 $\forall(v_i,v_j)\in E$（或 $\forall<v_i,v_j>\in E$），当且仅当 $(\varphi(v_i),\varphi(v_j))\in E'$（或 $<\varphi(v_i),\varphi(v_j)>\in E'$），称 G 与 G' **同构**。记作 $G\simeq G'$ 或 $G\cong G'$。

[理解] 图的同构是指可以通过调整结点位置和名称、边的形状和长短，但不改变结点和边之间的关联关系而使二者重合。或者说，同构是指两个图中的结点和边具有相同的邻接关系。

[定理 8-5] 两图同构存在如下的必要条件：

(1) 结点数目相同；

(2) 边数相同；

(3) 度数相同的结点数目相同；

(4) 对于一个图中的任一结点，在另一图中必然有度数相同的结点，且与二者相邻接结点的性质相同。

证明 略。

[辨析] 利用上述必要条件可以说明两图不同构，但不能肯定其同构。

例如，在图 8-6 中，$G_1 \simeq G_2$，$G_3 \simeq G_4$，$G_5 \simeq G_6$。以 G_1 和 G_2 为例，可以直接构造出同构映射 φ：$V_1 \to V_2$，满足

$$\varphi(a)=v_1,\ \varphi(b)=v_2,\ \varphi(c)=v_3,\ \varphi(d)=v_4,\ \varphi(e)=v_5。$$

不过，G_3 与 G_5 不同构，因为 G_3 中存在着彼此邻接的 3 个结点，但 G_5 至多只有 2 个结点邻接。

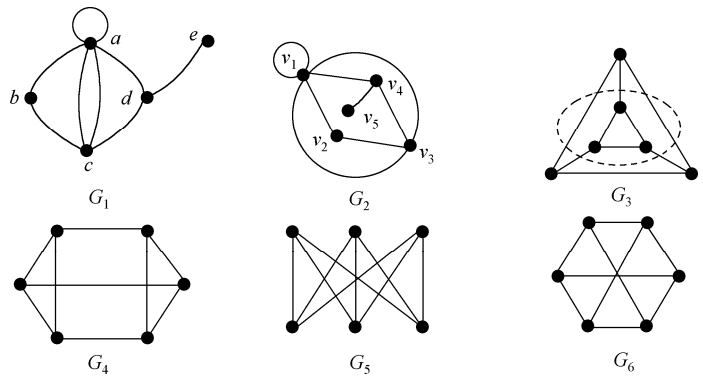


图 8-6

[延伸] 图的边是由一个起点和一个终点组成的，如果允许边由 2 个以上的结点组成则称为“超图”。超图可应用在数据可视化等领域[44, 45]。

思考与练习 8.1

8-1　解释零图、平凡图、简单图、完全图、正则图、子图、生成子图和补图的含义。

8-2　若图 $\overline{G}$ 是图 G 的补图，那么，图 G 也是图 $\overline{G}$ 的补图吗？

8-3　说明下述度序列是否可以构成无向图。

(a) 5,4,3,2,1,0。　(b) 2,2,2,2,2,2。　(c) 5,3,3,3,3,3。

(d) 3,3,3,2,2,2。　(e) 4,4,3,2,1。　(f) 4,4,3,3,3。

8-4　求出图 8-6 中 G_2 的 $\Delta(G_2)$ 和 $\delta(G_2)$。

8-5　设 G 是有 v 个结点 e 条边的无向图，证明 $\Delta(G) \geqslant 2e/v \geqslant \delta(G)$。

8-6　说明图 8-7 中的(a)与(b)不同构，但(c)与(d)同构。

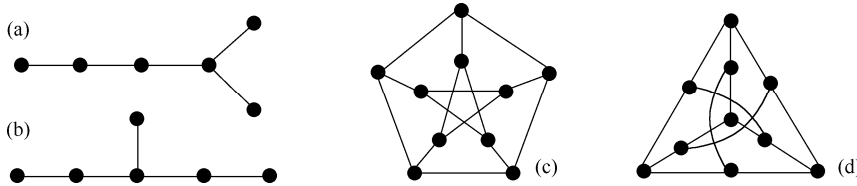


图 8-7

8-7 如果一个图同构于它的补图，则称其为自补图。给出一个 5 个结点的自补图。

8-8 判别是否存在 3 个或 6 个结点的自补图，并总结一个自补图对应的完全图的边数应满足的条件。

8-9 在任何一个人群中，总有 2 个人的朋友个数是相同的。建立适当的模型并证明此结论。

8.2 图的连通性

将一些代表目标的地点和道路分别看作图的结点和边，现实世界中经常要处理这样的问题，如何从一个图 G 中的给定结点出发，沿着一些边连续移动而达到另一指定结点。这种依次由点和边组成的序列，就形成了路以及连通的概念。两台计算机之间的通信就需要这样的一条路。

8.2.1 路与回路

[定义 8-10] 对于图 $G=<V,E>$，若有结点和边组成的交替序列 Γ：$v_0e_1v_1e_2v_2e_3\cdots e_mv_m$，其中，$e_i=(v_{i-1},v_i)\in E$ 或 $e_i=<v_{i-1},v_i>\in E$，$1\leqslant i\leqslant m$，则称 Γ 为连接 v_0 到 v_m 的**通路**（pass，或**路**）。这里的边数 m 称为通路的**长度**。v_0 和 v_m 分别称作通路的**起点**和**终点**，或统称为**端点**，其他结点称为**内部结点**。当 $v_0=v_m$ 且长度大于 0 时的通路称为**回路**（circuit）。

若一条通路中所有的边均不相同，则称作**简单（通）路**，也称为**迹**或**轨迹**（trail），$v_0=v_m$ 时的迹称为**简单回路**（或**闭迹**）。若一条通路中所有的结点各不相同则称作**路径**（path，或**基本通路**、**初级路**），$v_0=v_m$ 的路径称为**圈**（cycle）。

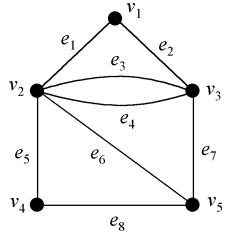


图 8-8

[辨析] 路径是迹，但迹不一定是路径，这是因为在一条路径中结点互不相同，从而所有的边一定互不相同。

例如，图 8-8 中存在的几种通路的示例如下：

通路（路）：$v_1e_1v_2e_3v_3e_4v_2e_6v_5e_8v_4$；

简单通路（迹）：$v_5e_8v_4e_5v_2e_6v_5e_7v_3$；

路径：$v_4e_5v_2e_6v_5e_7v_3e_2v_1$；

圈：$v_2e_3v_3e_7v_5e_8v_4e_5v_2$。

[辨析] 描述简单图中的通路没必要这么麻烦，因为它没有平行边，通常可以直接用结点序列表示为 Γ：$v_0v_1v_2\cdots v_m$，其中，$(v_{i-1},v_i)\in E$ 或 $<v_{i-1},v_i>\in E$，$1\leqslant i\leqslant m$。

[定理 8-6] 在一个 n 阶图中，如果存在一条从结点 u 到 v（$u\neq v$) 的通路，则必存在一条从 u 到 v 的不多于 $n-1$ 条边的路径。

证明 如果通路的长度多于 $n-1$，路中含有的结点数大于 n，必有重复结点，删除两结点间的边和结点仍是一条通路。重复此过程，删除所有重复结点后就得到了一条所求的路径。

[辨析] 不同书籍中关于路径、通路等概念的定义会有一些差异，如将通路定义为路，再将路径定义为通路等，主要原因是来自于对英文的不同表述，应注意鉴别。

8.2.2　无向图的连通性

1．连通与连通图

[定义 8-11] 在无向图 G 中，如果结点 u 和 v 之间存在一条通路，则称 u 和 v 是连通的。如果图 G 中任意两结点间都是连通的，则称 G 是**连通图**（connected graph）。

很明显，结点之间的连通关系 $R=\{<x,y>\mid x,y\in V$ 且x与y连通$\}$ 是结点集 V 上的等价关系（如果任何结点被认为与自己是连通的）。

[定义 8-12] 在无向图 G 中，利用连通关系 R 诱导出结点集 V 的划分，得到的等价类记作 V_1，V_2，…，V_m，所有 V_i 及其关联的边组成的子图 $G(V_i)$称为图 G 的**连通分支**（connected component），且记图 G 的**连通分支数**为 $W(G)$。

由等价关系的性质可知，两个结点 u 和 v 是连通的，当且仅当它们属于同一个连通分支。

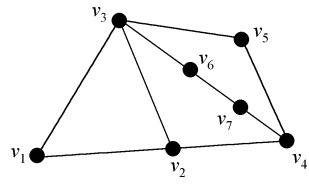


图 8-9

[辨析] 一个连通分支是指最大的连通子图，而不是一般的连通子图。例如，图 8-9 有一个连通分支，即本身是连通图，$\{v_2,v_3\}$ 可以组成连通子图，但不是连通分支，因为它不是最大连通子图。

[定义 8-13] 在无向图 G 中，如果结点 u 和 v 之间是**连通**的，则 u 和 v 之间的最短路径称为**短程线**，其长度（边数）称为 u 和 v 之间的**距离**，记作 $d(u,v)$。若 u 与 v 不连通，规定 $d(u,v)=+\infty$。

例如，图 8-9 中，有 $d(v_3,v_4)=2$。

结点间的距离 $d(u,v)$满足如下性质：

(1) $d(u,v)\geqslant 0$，当且仅当 $u=v$ 时等号成立；

(2) $d(u,v)=d(v,u)$；

(3) $d(u,v)+d(v,w)\geqslant d(u,w)$，称为三角不等式。

2．点割集与边割集

以下考虑图的连通性的“牢固程度”，即在图中删除结点或边对连通性的影响。需要注意的是，在图中删除一个结点时要同时删除其关联的边，但删除边时不删除其关联的结点。在图 G 中删除结点集合 V 记作 $G-V$，删除边集 E 记作 $G-E$。

[定义 8-14] 在无向图 $G=<V,E>$ 中，若有结点集 $V'\subseteq V$，使得 $W(G-V')>W(G)$，但图 G 删除了 V' 的任何真子集后，连通分支数不变，则称 V' 是 G 的一个**点割集**（cut-set of vertices）。若某一个结点构成一个点割集，则称该结点为**割点**（cut point）。

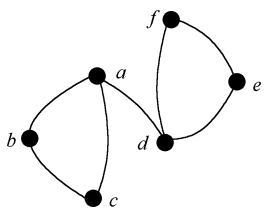


图 8-10

若有边集 $E'\subseteq E$，使得 $W(G-E')>W(G)$，而删除 E' 的任何真子集后，图 G 的连通分支数不变，则称 E' 是 G 的一个**边割集**（cut-set of edges）。若某一个边构成一个边割集，则称该边为**割边**或**桥**（bridge）。

例如，图 8-10 中的 a 和 d 为割点。边(a, d)为割边。

[定义 8-15] 若 G 是连通的无向图，且为非完全图，称 $\kappa(G)=\min\{|V'|\,|V'$ 是 G 的点割集$\}$为 G 的**点连通度**（或**连通度**，音/'kæpə/），$\lambda(G)=\min\{|E'|\,|E'$ 是 G 的边割集$\}$为 G 的**边连通度**（音/'læmdə/）。对平凡图和不连通图 G，有 $\kappa(G)=0$，$\lambda(G)=0$。

$\kappa(G)$ 是为了产生一个不连通图需要删去的最少结点数目，而 $\lambda(G)$ 是为了产生一个不连通图需要删去的最少边数。它们从不同角度刻画了连通程度，或者说连通性的强弱。

显然，存在割点的连通图的连通度 $\kappa(G)=1$，完全图 K_n 的连通度 $\kappa(G)=n-1$（删去 $n-1$ 个结点后变成平凡图）。存在割边的连通图的边连通度 $\lambda(G)=1$。

[定理 8-7] 对于任何一个无向图 G，有

$$\kappa(G)\leqslant\lambda(G)\leqslant\delta(G)。$$

证明 若 G 是不连通图或平凡图，有 $\kappa(G)=\lambda(G)=0\leqslant\delta(G)$。若 G 是完全图 K_n，则 $\kappa(G)=\lambda(G)=\delta(G)=n-1$。

对于其他情况，在删除最小度结点 v 所关联的全部边后，图 G 不连通，故 $\lambda(G)\leqslant\delta(G)$。当然，删除这些边关联的不同于 v 的 $\lambda(G)$ 个结点后也使图 G 不连通，故 $\kappa(G)\leqslant\lambda(G)$。结论成立。

例 8-4 若 n 阶简单图 G 的每一对结点度数之和大于等于 $n-1$，则 G 是连通图。

证明 若 G 不是连通图，不妨假设 G 包含两个连通分支 $G_1=<V_1,E_1>$ 和 $G_2=<V_2,E_2>$，其中 $|V_1|+|V_2|=n$。对 $\forall u\in V_1$ 和 $\forall v\in V_2$，必有 $\mathrm{d}(u)\leqslant|V_1|-1$，$\mathrm{d}(v)\leqslant|V_2|-1$，即 $\mathrm{d}(u)+\mathrm{d}(v)\leqslant n-2$，与题设矛盾。故 G 必是连通的。

8.2.3 有向图的连通性

无向图的连通性不能直接推广到有向图。

[定义 8-16] 在有向图 G 中，如果从结点 u 到 v 有一条路，称从 ***u* 可达 *v***。

可达性是有向图结点集上的二元关系，它是自反和传递的，但一般来说不是对称的。

有向图中可以类似地定义两个结点 u 和 v 之间的距离 $d(u,v)$。

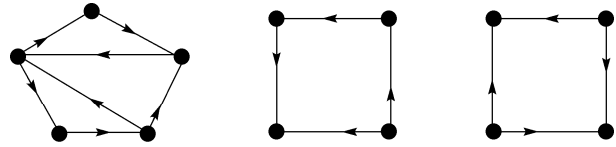
[定义 8-17] 设 G 是一个简单有向图，若略去所有边的方向后得到的无向图是连通的，则称 G 为**弱连通**的。若任意两个结点间至少从一个可达另一个，则称 G 是**单侧（向）连通**的。若任意两个结点间相互可达，则称 G 是**强连通**的。

容易理解，强连通图一定是单向连通图，单向连通图一定是弱连通图，反之不真。参见图 8-11。

可以通过下述方法判别强连通性：

[定理 8-8] 对一个有向图是强连通的，当且仅当 G 中有一条至少包含每个结点一次的回路。

证明 略。



强连通　　单向连通　　弱连通

图 8-11

思考与练习 8.2

8-10　解释通路、回路、路径、迹、圈、连通、强连通、弱连通、割点和割边的含义。

8-11　在图 8-12 所示的图 G 中，求出：

(a) 从 a 到 f 的所有通路。　(b) 从 a 到 f 的所有迹。

(c) a 到 f 的距离。　(d) $\kappa(G)$、$\lambda(G)$ 和 $\delta(G)$。

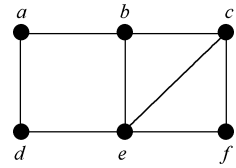


图 8-12

8-12　证明一个图 G 和它的补图 $\overline{G}$ 至少有一个是连通的。

8-13　若无向图中恰好有 2 个奇数度的结点，证明这 2 结点间必有一条通路。

8-14　设 G 是一个 n 阶简单无向图，且 $\delta(G)\geqslant n/2$，证明 G 是连通图。

8.3　图的矩阵表示

回顾已经了解的二元关系会发现，关系与有向图之间有着相同的“意义”。一个关系通过有向图得到关系图，而任何一个有向图也可以视为关系图，从而得到相应的关系。因此，关系中所描述的技术都可以应用于一般的图。

8.3.1　邻接矩阵

[定义 8-18] 若 $G=<V=\{v_1,v_2,\cdots,v_n\},E>$ 为简单图，则 n 阶方阵 $A(G)=[a_{ij}]_{n\times n}$ 称为 G 的**邻接矩阵**（adjacent matrix），其中

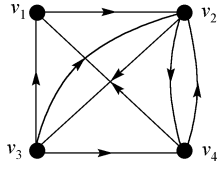


图 8-13

$$a_{ij}=\begin{cases}1 & ,(v_i,v_j)\in E\text{或}<v_i,v_j>\in E\\ 0 & ,\text{否则}\end{cases}。$$

上述定义中允许图中含有环。

显然，结点的邻接关系构成二元关系，而邻接矩阵就是关系矩阵。

例如，图 8-13 所示的图 G 具有如下的邻接矩阵：

$$A(G)=\begin{bmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&1&0&0\end{bmatrix}。$$

邻接矩阵中的两行和对应的两列同时对调相当于结点位置的交换，得到的矩阵描述了同样的有向图，只是相当于将结点的序号做了交换。

一个无向图的邻接矩阵是对称的，第 i 行的元素之和为结点 v_i 的度，其对角线元素 a_{ii} 表明结点 v_i 是否有环。有向图中第 i 行的元素之和为结点 v_i 的出度，而第 j 列的元素之和为结点 v_j 的入度。

[定理 8-9] 若 $A(G)=[a_{ij}]_{n\times n}$ 是图 $G=<V=\{v_1,v_2,\cdots,v_n\},E>$ 的邻接矩阵，则 $A(G)^m$ 中的元素 $a_{ij}^{(m)}$ 表示图 G 中由结点 v_i 到结点 v_j 的长度为 m 的通路数目。

证明 因为 $A(G)^2 = A(G)\cdot A(G)$，对于 $A(G)^2$ 中的任意元素 $a_{ij}^{(2)}$，有

$$a_{ij}^{(2)} = \sum_{k=1}^{n} a_{ik}\cdot a_{kj}。$$

由于每个 $a_{ik}\cdot a_{kj}$ 为 1 表示有一条由 v_i 经由 v_k 到 v_j 的长度为 2 的路，因此，$a_{ij}^{(2)}$ 为由结点 v_i 到结点 v_j 的长度为 2 的路的数目。由归纳法可知，$a_{ij}^{(m)}$ 表示图 G 中由结点 v_i 到结点 v_j 的长度为 m 的路的数目。

例如，对图 8-13 的图 G，有

$$A(G)^2 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 2 & 2 & 0 & 1 \\ 1 & 2 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix},\ A(G)^3 = \begin{bmatrix} 2 & 2 & 0 & 1 \\ 1 & 3 & 2 & 2 \\ 2 & 3 & 2 & 3 \\ 2 & 2 & 1 & 2 \end{bmatrix},\ A(G)^4 = \begin{bmatrix} 1 & 3 & 2 & 2 \\ 4 & 5 & 3 & 5 \\ 5 & 7 & 3 & 5 \\ 3 & 5 & 2 & 3 \end{bmatrix}。$$

根据计算结果可知，由结点 v_3 到结点 v_4 有 3 条长度为 3 的路，有 5 条长度为 4 的路。

通常，我们并不关心由结点 v_i 到结点 v_j 有什么样的路，而仅是关心是否可由 v_i 到达 v_j。

[定义 8-19] 若 $G=<V=\{v_1,v_2,\cdots,v_n\},E>$ 为简单图，则 n 阶方阵 $P(G)=[p_{ij}]_{n\times n}$ 称为 G 的**可达矩阵**（reachable matrix），其中

$$p_{ij} = \begin{cases} 1 & ,v_i\text{可达}v_j \\ 0 & ,\text{否则} \end{cases}。$$

显然，计算可达矩阵可以先计算 $B=\sum_{k=1}^{n} A(G)^k$，将 B 中所有非零元素置为 1 即为 $P(G)$。或者，直接采用逻辑加法求出可达矩阵 $P(G)=\bigvee_{k=1}^{n} A(G)^k$。

可达矩阵恰好是关系的传递闭包的关系矩阵，经典的快速计算方法就是采用 4.4 节中讨论的 Warshall 算法。

例如，图 8-13 的图 G 的可达矩阵为

$$P(G)=\bigvee_{k=1}^{n} A(G)^k = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}。$$

可见，这是一个强连通图。

任何一个结点到自身的可达性存在两种处理方法，其一是认为有环可达，否则不可达，此即本书的定义。另一种方法是认为任何结点到自身总是可达的，与环的有无无关。此时，总有 $p_{ii}=1$，$1\leqslant i\leqslant n$。

8.3.2 关联矩阵

还可以采用关联矩阵来表示一个图。

[定义 8-20] 若 $G=<V=\{v_1,v_2,\cdots,v_n\},E=\{e_1,e_2,\cdots,e_m\}>$ 为图，则 n 行 m 列矩阵 $M(G)=[m_{ij}]_{n\times m}$ 称为**关联矩阵**（incidence matrix）或**完全关联矩阵**。若 G 为无向图，则

$$m_{ij}=\begin{cases}1 & ,v_i\text{关联}e_j\\ 0 & ,\text{否则}\end{cases}。$$

若 G 为有向图，则

$$m_{ij}=\begin{cases}1 & ,v_i\text{为}e_j\text{的起点}\\ -1 & ,v_i\text{为}e_j\text{的终点}\\ 0 & ,v_i\text{与}e_j\text{不关联}\end{cases}。$$

例如，对于图 8-14 中的图 G，其关联矩阵为：

$$M(G)=\begin{bmatrix}1&-1&0&0&0&-1&1\\0&1&-1&0&0&0&0\\0&0&1&1&-1&1&-1\\-1&0&0&-1&1&0&0\end{bmatrix}。$$

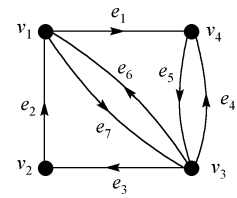


图 8-14

对于无向图的关联矩阵，有

(1) 因每条边关联 2 个结点（环的两个关联结点重合），故各列元素和为 2，即 $\sum_{i=1}^{n}m_{ij}=2$。

(2) 各行元素和等于结点的度，即 $\sum_{j=1}^{m}m_{ij}=\mathrm{d}(v_i)$。

对于有向图的关联矩阵，有

(1) 由于每条边贡献一个出度和入度，故各列元素和、所有元素和为 0，即 $\sum_{i=1}^{n}m_{ij}=0$，$j=1,2,\cdots,m$，且 $\sum_{j=1}^{m}\sum_{i=1}^{n}m_{ij}=0$。

(2) 第 i 行中 1 的个数为 v_i 的出度，-1 的个数为 v_i 的入度，$i=1,2,\cdots,n$。

思考与练习 8.3

8-15　写出图 8-15 中图 G 的邻接矩阵 A，找出从 v_1 到 v_4 长度为 2 和 4 的通路，并计算 A^2 和 A^4 以验证你的结论。

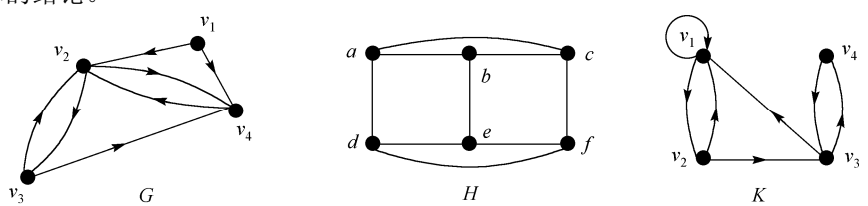


图 8-15

8-16 写出图 8-15 中的图 H 的完全关联矩阵。

8-17 写出图 8-15 中的图 K 的邻接矩阵，并计算：

(a) 从 v_1 到 v_4 的长度分别为 1、2、3、4 的通路数目。

(b) 从 v_1 到自身的长度为 1、2、3、4 的回路数目。

(c) 长度为 4 的回路数目和非回路的通路数目。

(d) 可达矩阵。

8.4 二部图、欧拉图与汉密尔顿图

8.4.1 二部图

很多应用中的对象可以按性质不同分组，同组的对象之间没有关联，即关联仅发生在不同组的对象之间。例如，一组工人与一组任务的工作分配、一组学生与一组课程的选课应用、一组课程与一组教室的排课系统等均属此类。对这些问题的抽象结果形成了一类特殊的图，即二部图。

[定义 8-21] 若无向图 $G=<V,E>$ 的结点集 V 可分为两个不相交的子集 V_1 和 V_2，使得对 $\forall(u,v)\in E$，有 $u\in V_1$，且 $v\in V_2$，则称 G 为**二部图**（或**偶图**，或**二分图**）（bipartitegraph 或 bigraph）。二部图也可记为 $G=<V_1,V_2,E>$。

如果 V_1 中每个结点都与 V_2 中的所有结点邻接，则称 G 为**完全二部图**，并记为 $K_{|V_1||V_2|}$。

例如，图 8-16 显示了 1 个普通二部图，2 个完全二部图 $K_{2,3}$ 和 $K_{3,3}$。

可依据如下结果判别一个图是否为二部图：

[定理 8-10] 无向图 $G=<V,E>$ 是二部图，当且仅当 G 的所有回路的长度为偶数。

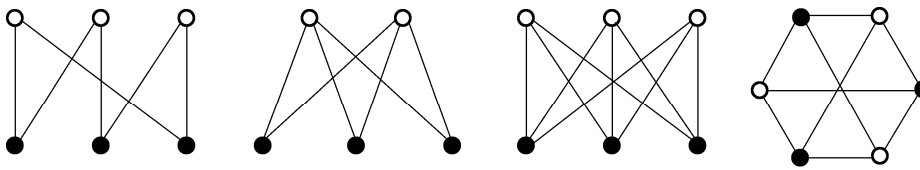


图 8-16

证明 必要性。若 $G=<V_1,V_2,E>$ 为二部图，记 $v_1v_2\cdots v_kv_1$ 是 G 中一条长度为 k 的回路。不妨设 $v_1\in V_1$，因 v_2 与 v_1 相邻，故 $v_2\in V_2$。同样，$v_3\in V_1$，等等。即 $v_{2i+1}\in V_1$，$v_{2i+2}\in V_2$，$i\geqslant 0$。故回路的长度必是偶数。

充分性。设 G 中的每条回路长度都是偶数。若 G 为零图，结论显然成立。这里假定 G 为连通图（否则可对每个连通分支证明），则可任取 $u\in V$，利用如下规则将结点分组：

$$V_1=\{v\in V\wedge d(u,v)\text{为偶数}\},$$

$$V_2=\{v\in V\wedge d(u,v)\text{为奇数}\}。$$

那么，$V_1 \cap V_2 = \varnothing$，$V_1 \cup V_2 = V$，且至少 $u \in V_1$，与 u 邻接的结点 $\in V_2$，即 $V_1 \neq \varnothing$，$V_2 \neq \varnothing$。以下说明 V_1 中的任意两结点均不相邻。否则，不妨设有 $v_i, v_j \in V_1$，二者相邻，即边 $(v_i, v_j) \in E$。记 u 到 v_i、u 到 v_j 的短程线分别为 C_1 和 C_2，显然，C_1、C_2 和边 (v_i, v_j) 构成经由 u、v_i 和 v_j 的回路，参见图 8-17，且长度为奇数，与已知矛盾。同理，V_2 中的结点之间也不相邻。故 G 是二部图。

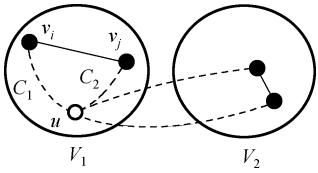


图 8-17

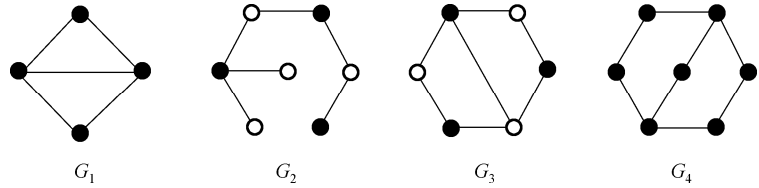


图 8-18

例如，图 8-18 中的 G_1 和 G_4 不是二部图，因为它们都含有长度为奇数的回路，而 G_2 和 G_3 是二部图。

二部图是一种应用广泛的图结构，其核心问题之一是匹配问题。

[定义 8-22] 在无向图 $G = <V, E>$ 中，$M \subseteq E$，若 M 中任意两条边均不相邻，则称 M 是 G 中的一个**匹配**（matching，或**边独立集**，或**对集**）。若在 M 中增加任何新边都不再是匹配，则称 M 是**极大匹配**。边数最多的极大匹配称为**最大匹配**。

例如，图 8-16 中各图 G、$K_{2,3}$ 和 $K_{3,3}$ 的最大匹配的边数分别为 3、2 和 3，且可以看出，最大匹配并不是唯一的。

如果有一组教师和一组课程，每位教师都可以任意选择只教授一门课程，那么，自然可以将问题用二部图来描述，且任意一个最大匹配就给出了一个所有教师能够承担最多门课程的具体方案。

例 8-5　设有 3 个课外小组，分别为网游设计、ACM 竞赛和物联网，有 5 个学生 s_1，s_2，s_3，s_4 和 s_5。已知：

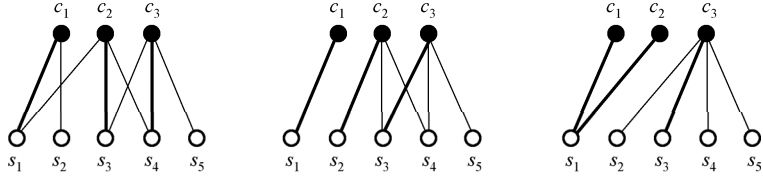
(1) s_1，s_2 为网游设计组成员；s_1，s_3，s_4 为 ACM 竞赛组成员；s_3，s_4，s_5 为物联网组成员。

(2) s_1 为网游设计组成员；s_2，s_3，s_4 为 ACM 竞赛组成员；s_2，s_3，s_4，s_5 为物联网组成员。

(3) s_1 同时为网游设计和 ACM 竞赛组成员；s_2，s_3，s_4，s_5 为物联网组成员。

问：可否针对上述 3 种不同情况，在 5 名学生中选 3 位不兼职的组长？

解　将课外小组用 c_1，c_2，c_3 表示。若 s_i 是 c_j 的成员，则添加一条边 (s_i, c_j)。于是，得到 3 种情况的二部图，参见图 8-19。



(1)　(2)　(3)

图 8-19

由图可知，情况(1)和(2)都有多种选出方案。例如，情况(1)中还可选 s_2， s_4 和 s_5 分别担任 3 组的组长。不过，情况(3)无法按要求选出 3 组组长。

[延伸] 二部图可以有效地解决如人员分配、教室排课及其各种网络模型中存在的问题。在人工神经网络中，输入层与隐含层、隐含层与隐含层之间也多为二部图结构[46-48]。

8.4.2 欧拉图

18 世纪中叶，东普鲁士的哥尼斯堡城（今俄罗斯的加里宁格勒）被一条贯穿全城的普雷格尔河分为 4 块，但可通过 7 座桥彼此相连，参见图 8-20(a)。当时该城的居民热衷于探讨这样一个游戏：从任何一块陆地出发，按什么路线可以经过每座桥一次且仅一次而回到原地？这就是著名的哥尼斯堡七桥问题。

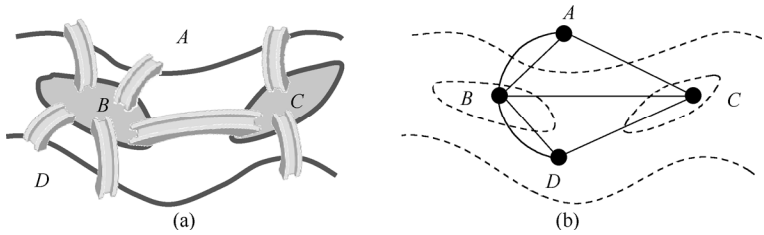


图 8-20

1736 年，著名的瑞士数学家欧拉（Leonhard Eulerian）研究并给出了七桥问题的答案：无解，即不存在这样的路线。

欧拉将上述问题用一个抽象的图形来描述，其中的 4 块陆地分别用 4 个点表示，连接陆地之间的桥用连接两点的边表示，就得到了图 8-20(b)的简化图。于是，该问题变成了：能否在图 G 中找到一条通过每条边一次且仅一次的回路呢？

[定义 8-23] 给定无孤立结点的无向图 G，G 中经过每条边一次且仅一次的通路（回路）称为**欧拉路**（**欧拉回路**）。具有欧拉回路的图称为**欧拉图**（Eulerian graph）。

[辨析] 尽管欧拉回路是欧拉路，但有欧拉路不能保证有欧拉回路，只有欧拉路而无欧拉回路的图也不能称为欧拉图。

可以这样判别一个图中是否含有欧拉路以及是否为欧拉图：

[定理 8-11] 无向图 G 具有一条欧拉路，当且仅当 G 是连通的，且有零个或两个奇数度结点。图 G 具有欧拉回路，当且仅当 G 是连通的且所有结点度数全为偶数。

证明 必要性。若 n 阶图 G 具有欧拉路，则有路 $v_1v_2\cdots v_l$ 经过每条边，$l \geqslant n$， v_i 可能重复。因为无孤立点，每结点至少连接一条边，故 $v_1v_2\cdots v_l$ 中一定包含了图的所有结点，可见 G 必然连通。由于每个非端点的结点 v_i 必在欧拉路中出现，而每次出现必关联两条边，故 $\mathrm{d}(v_i)$ 是偶数。可见，若 $v_1 = v_l$，则所有结点的度为偶数，否则，只有度 $\mathrm{d}(v_1)$ 和 $\mathrm{d}(v_l)$ 为奇数，其余结点的度均为偶数。

充分性。若 G 是连通的，且有零个或两个奇数度结点 v_1 和 v_l。若无奇数度结点，任选一个结点做 v_1。以 v_1 为起点，这样构造一条欧拉路或回路：

从 v_1 出发构造一条迹，即沿一关联边到达结点 v_2。因为 $\mathrm{d}(v_2)$ 为偶数，必可沿另一边到达 v_3。重复此过程，直到另一个奇数度结点 v_l 或 v_1，得到一条迹或闭迹 T_1。

若 T_1 通过 G 的所有边，则 T_1 就是欧拉路或欧拉回路。否则，T_1 中必存在结点 v_i 满足 $\mathrm{d}_{T_1}(v_i) < \mathrm{d}(v_i)$，这里的 $\mathrm{d}_{T_1}(v_i)$ 为 v_i 在子图 T_1 中的度。在 G 中去掉子图 T_1，从 v_i 出发按前述方法找到新的迹 T_2。

若组合 T_1 和 T_2 得到 G 则结束。否则，继续此过程直到得到最终的欧拉路。图 8-21 显示了构造欧拉路时的合并过程。

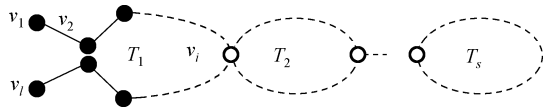


图 8-21

[辨析] 如前文定义的那样，迹就是指边不重复的路。欧拉（回）路的构造就是利用小回路合并成最终（回）路的过程。

欧拉路和欧拉回路都可以推广到有向图中。

[定义 8-24] 给定无孤立结点的有向图 G，G 中经过每条边一次且仅一次的单向路（回路）称为**单向欧拉路**（**欧拉回路**）。具有单向欧拉回路的图称为（有向）**欧拉图**。

[定理 8-12] 有向图 G 具有一条单向欧拉回路，当且仅当 G 是连通的，且所有结点的入度等于出度。单向欧拉路只有两个结点除外，且其中一个出度比入度大 1，另一个入度比出度大 1。

例 8-6　判别图 8-22 中的图是否为欧拉图。

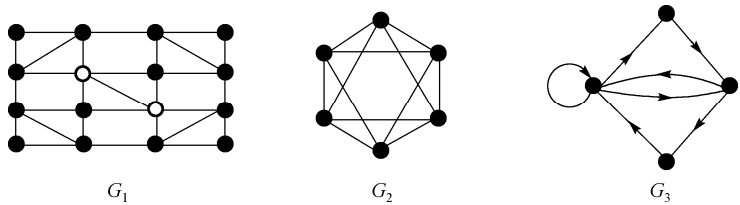


图 8-22

解　图 G_1 中只有 2 个奇数度结点，有欧拉路但无欧拉回路，不是欧拉图。G_2 和 G_3 都是欧拉图。

判别一个图 G 是否为欧拉图也就是“一笔画问题”，即笔不离纸，每条边只画一次而不许重复地将图一笔画出。

[延伸] 存在一个较有名的求欧拉路的算法称为 Fleury 算法[48]。

[延伸] 一个无向图（甚至有向图）的边可以赋予一组数值，表示边的长度，以代表实际长度、费用和时间等。这种图称为带权图，且无向带权图也称为网络。

欧拉路仅关心是否有一条路，而在网络中有时更希望了解哪条欧拉路是最短的，这样的问题称为“中国邮路问题”[48]。

8.4.3 汉密尔顿图

1859 年，爱尔兰的威廉·汉密尔顿（William Hamiltonian）爵士发明了一个小游戏，在一个正十二面体的结点上标记 20 个城市，游戏的目的是沿十二面体的边寻找一条路能够通过所有城市，且每个城市只通过一次，最后返回原地。汉密尔顿称此问题为“周游世界问题”，并做了肯定的回答。图 8-23 给出了一条周游路线。

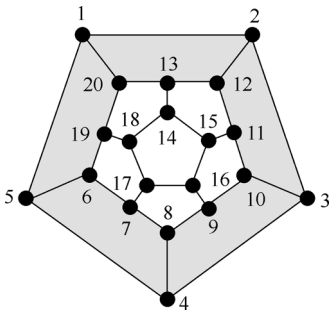


图 8-23

[定义 8-25] 通过图中每个结点一次且仅一次的路（回路）称为**汉密尔顿路**（**汉密尔顿回路**）。具有汉密尔顿回路的图称为**汉密尔顿图**（Hamiltonian graph）。规定平凡图为汉密尔顿图。

[辨析] 汉密尔顿回路是经过所有结点的最短回路。一条汉密尔顿路就是图的所有结点的一个全排列。

因为一个图中的平行边和环不影响是否存在汉密尔顿路和回路，故可以仅考虑简单图。同时，汉密尔顿路的定义对无向图和有向图都适用。

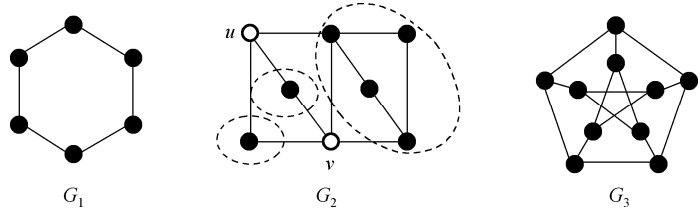
与欧拉图不同，目前仍没有判别汉密尔顿图的充分必要条件，但可以分别给出充分条件和必要条件。

[定理 8-13] 在 n 阶简单图 G 中，若 G 的每一对结点度数之和大于等于 $n-1$，则 G 中存在汉密尔顿路。若 G 的每一对结点度数之和大于等于 n，则 G 中存在汉密尔顿回路。

证明 略。

[延伸] 此定理存在两种证法，包括反证法和构造性证法[48]。

此定理是充分而非必要的，即一个汉密尔顿图并非一定要满足定理的要求。例如，图 8-24 中的 6 阶图 G_1 是汉密尔顿图，但两个结点的度数和为 4<6−1。



G_1 G_2 G_3

图 8-24

利用上述定理可以判定一些特殊的图是汉密尔顿图：

(1) 若 n 阶（$n\geqslant 3$）无向简单图 G 的最小度 $\delta(G)\geqslant n/2$，则 G 是汉密尔顿图。

(2) 完全图 K_n（$n\geqslant 3$）和完全二部图 $K_{n,n}$（$n\geqslant 2$）是汉密尔顿图。

利用下面的必要条件可以肯定一个图不是汉密尔顿图：

[定理 8-14] 若图 $G=<V,E>$ 是汉密尔顿图，则对结点集 V 的每个非空子集 S 均有 $W(G-S)\leqslant|S|$，其中的 $W(G-S)$ 是 $G-S$ 的连通分支数。

证明　设 C 是 G 的一条汉密尔顿回路，$S=\{s_1,s_2,\cdots,s_m\}$ 为 V 的非空子集。对 $\forall s_1\in S$，在 C 中删去 s_1 后的图 $G-\{s_1\}$ 仍连通，即 $W(C-\{s_1\})=1$。再删去 s_2 至多形成 2 个连通分支，即 $W(C-\{s_1,s_2\})\leqslant 2$。利用归纳法可知，有

$$W(C-S)\leqslant |S|。$$

由于 C 是 G 的生成子图，G 一般比 C 有更多的边，或者说 G 比 C 有更强的连通性，即 $W(G-S)\leqslant W(C-S)$，故结论成立。

由定理可知，有割点的图一定不是汉密尔顿图。这是因为若 v 是图 G 的割点，则 $W\left(G-\{v\}\right)=2$。

例如，图 8-24 中的 G_2 不是汉密尔顿图，因为 $W(G-\{u,v\})=3$。

此定理是必要但不是充分的，这就是说，即使 $W(G-S)\leqslant |S|$ 成立也可能不是汉密尔顿图。例如，图 8-24 中的 G_3 就满足此条件，但它不是汉密尔顿图。此图称为“彼得森（Petersen）图”。

[延伸] 与中国邮路问题类似，在一个网络中经常要计算哪条汉密尔顿路是最短的，这样的问题称为“巡回售货员”问题或“货郎担”问题[48]。

[延伸] 无论是欧拉路还是汉密尔顿路，并非不存在求解算法。例如，可以将所有边或结点进行全排列后逐个进行检验，这样的算法在边或结点很多时耗费时间巨大。因此，这些问题求解的核心是寻找效率更高的算法[48]。

思考与练习 8.4

8-18　判断图 8-25 中的图(a)和(b)是否为欧拉图。

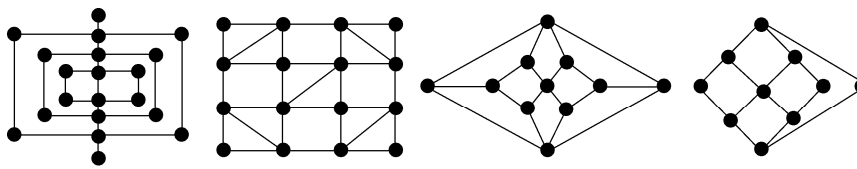


图 8-25

8-19　判断图 8-25 中的图(c)和(d)是否为汉密尔顿图。

8-20　对哪些 m 和 n，完全二部图 $K_{m,n}$ 中分别存在欧拉回路和欧拉路？

8-21　对哪些 n，完全图 K_n 中存在欧拉回路？

8-22　证明具有奇数个结点的二部图没有汉密尔顿回路。

8-23　设有 7 个人分别是 a、b、c、d、e、f、g，他们各擅长一些语言：

(a) a 会讲英语。　(b) b 会讲英语和汉语。

(c) c 会讲英语、意大利语和俄语。　(d) d 会讲日语和汉语。

(e) e 会讲德语和意大利语。　(f) f 会讲法语、日语和俄语。

(g) g 会讲法语和德语。

问可否从这 7 人中找出 7 名翻译，使每个人翻译一种不同的语言？

8-24 设有简单图 G，其结点数和边数为 $v \geqslant 3$ 和 e，且 $e \geqslant \binom{v-1}{2} + 2$，证明 G 是汉密尔顿图。

8.5 平 面 图

8.5.1 平面图与欧拉定理

在一些特殊的应用如印刷电路板布线、管道设计等抽象出来的问题中，通常希望图的边没有交叉，这样的图就是平面图。一般平面图仅指无向图。

[定义 8-26] 如果能把一个无向图 G 画在平面上，且任何两条边除了端点外没有其他交点，称 G 是一个**平面图**（plane graph）。

例如，图 8-26 中的 G_1 改画成 G_2 后可知其为平面图，而 $K_{3,3}$ 无论如何改造（如 G_3）总会有边交叉，不是平面图。

[辨析] 将一个图改画成平面图更体现了拓扑意义，你可以随意重新安排结点的位置或拉伸、弯曲任何一条边。

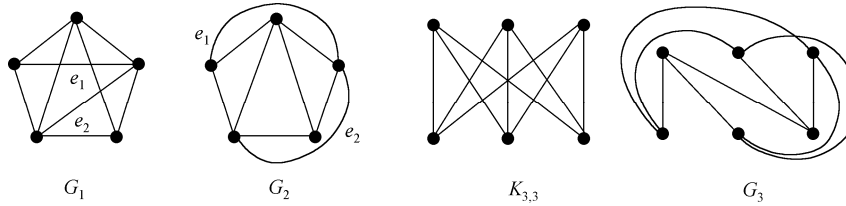


图 8-26

[定义 8-27] 设 G 是平面图，由 G 的边将 G 所在的平面划分为若干区域，各区域内不包含边和结点，则每个区域称为 G 的一个**面**（face）。面积有限的面称作**有限面**或**内部面**，面积无限的面称作**无限面**或**外部面**。

包围一个面的边构成回路，称为面的**边界**。面 r 的边界长度称为该面的**次数**，记作 $\deg(r)$。若两个面至少有一条公共边，则称其为**邻接面**。

例如，图 8-27 中的图共有 5 个面 r_0，r_1，r_2，r_3，r_4。其中，r_0 是无限面，r_4 由 4 条边围成，而 r_3 相当于由 5 条边所围成，即 $\deg(r_0)=3$，$\deg(r_1)=3$，$\deg(r_2)=3$，$\deg(r_3)=5$，$\deg(r_4)=4$。

面 r_3 有些特殊，它是这样围成的：从结点 c 开始，沿边(c,d)、(d,e)、(e,f)、(f,e)、(e,c)构成回路，形成该面。其中，特殊的边(e,f)正反各走一次。

[辨析] 显然，无向图仅有一个无限面。可以想象整个图包围在一个圆或矩形内，以免遗漏这个面。

[辨析] 若简单图的结点数 $v \geqslant 3$，且边数 $e \geqslant 3$，则对每个面 r 有 $\deg(r) \geqslant 3$，即除了特殊情况外，一个面至少由 3 条边围成。

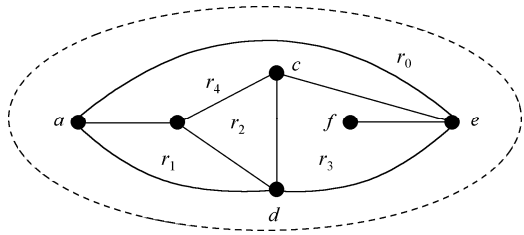


图 8-27

平面图的边和面的次数有着非常简单的关系：

[定理 8-15] 任何一个有限平面图的面的次数之和等于其边数的 2 倍，即

$$\sum_{i=1}^{r}\deg(r_i)=2e。$$

其中的 r 和 e 分别为面数和边数。

证明　因为任何一条边，或者是两个面的公共边，或者在一个面中作为边界被计算 2 次，如图 8-27 中的边(e,f)，故面的次数之和等于其边数的 2 倍。

[定理 8-16] 设 G 是连通平面图，共有 v 个结点，e 条边和 r 个面，则有如下**欧拉公式**：

$$v-e+r=2。$$

此定理称为**欧拉定理**。若 G 是有 k 个连通分支的平面图，则推广的欧拉公式为

$$v-e+r=k+1。$$

证明　对边采用归纳法。若 G 无边，即 G 为平凡图，则 $v=1$，$e=0$，$r=1$，可知结论成立。若 G 仅有一条边，则 $v=2$，$e=1$，$r=1$，结论也成立。

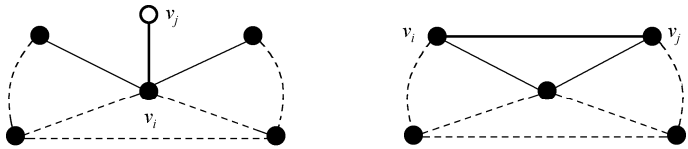


图 8-28

若 G 有 e 条边时欧拉公式成立，$v-e+r=2$。当 G 有 e+1 条边时，新增的边只有图 8-28 所示的两种可能的加入方法。对于情况 1，图的结点数 v 和边数 e 各增 1，面数 r 不变，有

$$(v+1)-(e+1)+r=2。$$

对于情况 2，图的结点数 v 未变，边数 e 和面数 r 各增 1，有

$$v-(e+1)+(r+1)=2。$$

可见欧拉定理成立。

当 G 由 k 个连通分支组成时，对于每个连通分支，单独作为平面图看待时有

$$v_i - e_i + r_i = 2。$$

其中的 v_i、e_i 和 r_i 为其结点数、边数和面数。于是，有

$$\sum_{i=1}^{k}(v_i - e_i + r_i) = 2k = v - e + \sum_{i=1}^{k} r_i。$$

由于每个连通分支有一个外部面，而合并后的图 G 只有一个外部面，即 $r = \sum_{i=1}^{k} r_i - (k-1)$，代入后即得到推广的欧拉公式。

[辨析] 欧拉公式源自于有关空间中多面体的欧拉定理，其中的 v 是结点数，e 为棱数，r 为面数，两个定理的内容相同。

例 8-7 若 G 是一个有 v（$v \geqslant 3$）个结点、e 条边的简单连通平面图，则有

$$e \leqslant 3v - 6。$$

证明 记 G 的面数为 r。若 $v = 3$，$e = 2$，结论显然成立。若 $e \geqslant 3$，每个面的次数不小于 3。因为所有面的次数和为边数的 2 倍，即 $2e \geqslant 3r$。代入欧拉定理，有

$$2 = v - e + r \leqslant v - e + 2e/3。$$

整理后就是 $e \leqslant 3v - 6$。

此结果可作为定理使用。有时，利用上述结果判定一个图不是平面图比欧拉定理更直接。例如，对完全图 K_5，$v = 5$，$e = \binom{5}{2} = 10$，有 $3v - 6 = 9 < e$，故 K_5 不是平面图。

例 8-8 证明完全二部图 $K_{3,3}$ 不是平面图。

证明 若完全二部图 $K_{3,3}$ 是平面图，因为 $K_{3,3}$ 中同一组的结点不邻接，故每个面的次数不小于 4。因此，$2e \geqslant 4r$，即 $r \leqslant e/2$。由欧拉定理，必有

$$2 = v - e + r \leqslant v - e + e/2 = v - e/2。$$

即 $2v - 4 \geqslant e$。但由于 $v = 6$，$e = 9$，显然不满足此不等式，故 $K_{3,3}$ 不是平面图。

[延伸] 利用欧拉定理否定平面图是有效的，但并没有简单的方法证明其是平面图。不过，存在一个可用的库拉托夫斯基（Kuratowski）定理[48]。

8.5.2 平面图的对偶图

[定义 8-28] 设平面图 $G = < V, E >$ 的结点数、边数和面数分别是 v、e 和 r，其各个面记为 r_i，$1 \leqslant i \leqslant r$。按如下方法构造图 $G^* = < V^*, E^* >$ 并称其为 G 的**对偶图**（dual graph）：

(1) 在图 G 的每个面 r_i 内任取一点 v_i^* 作为 G^* 的结点，得 $V^* = \{v_i^* \mid 1 \leqslant i \leqslant r\}$。

(2) 若面 r_i 和 r_j 的边界中有公共边 e_k，连接 v_i^* 和 v_j^* 与 e_k 相交，构成 G^* 的边 e_k^*。

(3) 若 e_k 仅是一个面 r_i 的边界，则以 v_i^* 为结点做环 e_k^* 作为 G^* 的环，得 $E^* = \{e_i^* \mid 1 \leqslant i \leqslant e\}$。

例如，用实心圆和实线表示图 G 的结点和边，用空心圆和虚线表示对偶图 G^* 的结点和边，则图 8-29 显示了图 G_1、G_2 及其对偶图 G_1^* 和 G_2^*。

[辨析] 粗略地说，对于一个平面图 G，将面聚为结点，任意两结点间穿过 G 的边连线，就得到了 G 的对偶图 G^*。

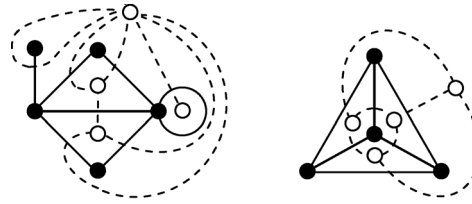


图 8-29

[辨析] 对偶是相互的，若 G^* 是 G 的对偶图，则 G 也是 G^* 的对偶图。

由结点、边数和面数的关系可以看出，平面图的对偶图仍然是平面图。不过，一个平面图 G 与其对偶图通常不是同构的。

[定义 8-29] 若平面图 G 与其对偶图 G^* 同构，称 G 是**自对偶图**。

[理解] 这个定义的含义是：自对偶图 G 的对偶图就是自己。

例如，图 8-29 中的 G_2 就是一个自对偶图。

8.5.3　平面图的着色

1852 年，英国的弗南西斯·格思里（Francis Guthrie）提出了一个假设：每幅地图都可以用四种颜色着色，使得有共同边界的国家着上不同的颜色，这就是“四色猜想”。1880 年，肯普提出了一种可以证明地图可用 5 种颜色着色的办法。1976 年，美国的两位数学家利用计算机完成了四色猜想的证明，进而将其命名为四色定理。

图的（结点）着色是指，若 G 为平面图，对 G 的每个结点都指定一种颜色，使得没有两个相邻结点指定为相同颜色。

[定义 8-30] 若图的结点着色的 k 种颜色选自一个有 k 种颜色的集合（不管 k 种颜色是否都用到），则称为图的结点 ***k* 着色**或 ***k* 可着色**。图 G 的结点着色所需要的最小颜色数称为 G 的**色数**，记作 $\chi(G)$（音/kai/）。同时，$\chi(G)=k$ 的图称为 ***k* 色图**。

[辨析] $\chi(G)=k$ 是指 G 是 k 可着色，但不是 k–1 可着色的。

[定理 8-17] 对于零图 G，有 $\chi(G)=1$；对于任意二部图 G，有 $\chi(G)=2$；对于 n 阶完全图 K_n，有 $\chi(K_n)=n$。

结论是显然的。

目前，并没有简单的方法能够证明一个图 G 是否为 n 可着色的，但可以尝试用韦尔奇·鲍威尔（Welch Powell）方法进行着色：

(1) 将图 G 的结点按度数递减排序；

(2) 用颜色 1 对第一点着色，并按序对其后的与前面着色点不相邻的每点着相同颜色；

(3) 逐个用以后的颜色对尚未着色的点重复(2)，直到对所有点着色。

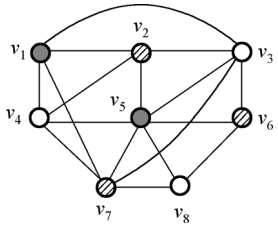


图 8-30

例 8-9 利用韦尔奇·鲍威尔法对图 8-30 中的图 G 着色。

解 先对结点按度排序为 v_5，v_3，v_7，v_1，v_2，v_4，v_6，v_8。用颜色 1 对第一点 v_5 着色，并对与其不相邻的结点 v_1 着色。其次，用颜色 2 对 v_3 及其不相邻的 v_4 和 v_8 着色。最后，用颜色 3 对 v_7 及其不相邻的 v_2 和 v_6 着色，则所有结点均被着色。由于 v_5、v_7 和 v_8 相互邻接，即 G 不能是 2 可着色的。因此，$\chi(G)=3$。

图的色数可被用来解决某些实际问题。例如，若某高校有 n 门选修课要进行期末考试，同一名学生一天至多只能参加一门课程考试，那么，期末考试需要几天？

记选修课为结点集合 $V=\{v_1, v_2, \cdots, v_n\}$，构造简单图 $G=<V, E>$，$(v_i, v_j)\in E$ 当且仅当 v_i 和 v_j 被同一名学生选修。那么，图 G 的色数 $\chi(G)$ 就是所需的最少天数。

[定理 8-18] 对任意平面图 G，有 $\chi(G)\leqslant 4$。

此即**四色定理**，但尚无简单的证明方法。

思考与练习 8.5

8-25 若一个 7 阶连通平面图有 6 个面，求出它的边数。

8-26 若一个具有 3 个连通分支的平面图有 4 个面和 9 条边，求出它的阶数。

8-27 画出图 8-31 中各图的对偶图。

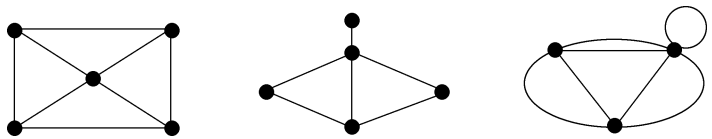


图 8-31

8-28 求出图 8-31 中各图的色数。

8-29 若一个 n 阶连通平面图 G 有 m 条边，每个面的次数至少为 4，证明 $m\leqslant 2n-4$。

8-30 设 v 阶图 G 是自对偶平面图，且有 e 条边，证明 $e=2v-2$。

8-31 证明：若有 e 条边的 v 阶连通平面图 G 的每个面的次数至少为 k（$k\geqslant 3$），则 $e\leqslant k(v-2)/(k-2)$，并由此说明图 8-24 中的彼得森图是非平面图。

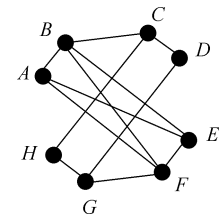


图 8-32

8-32 若简单连通平面图 G 的最小度 $\delta(G)\geqslant 3$，证明其边数不可能为 7。

8-33 利用韦尔奇·鲍威尔法对图 8-32 进行着色并求出其色数。

8.6　树

8.6.1　无向树

这里仅讨论无向图中的树。

[定义 8-31] 连通且无回路的图称为**无向树**，简称为**树**（tree）。树中度为 1 的结点称为**叶**或**树叶**（leaf），度大于 1 的点称为**分支点**或**内点**（internal vertice）。一棵树的结点个数称为树的**阶数**。

一个无回路的无向图，如果它的每个连通分支都是树则称为**森林**（forest）。

[定理 8-19] 对于给定的有 v 个结点和 e 条边的图 $T=<V,E>$，以下关于树的定义等价：

(1) 无回路的连通图，即 G 是树。

(2) 无回路且 $e=v-1$。

(3) 连通且 $e=v-1$。

(4) 无回路，但增加一条新边将产生唯一一条回路。

(5) 连通，但删去任一边后不再连通。

(6) 每对结点之间有且仅有一条路。

证明　(1)⊢(2)。$v=2$ 时显然成立。假设 $v=k$ 时命题成立，当 $v=k+1$ 时，因为图连通且无回路，至少存在一个度为 1 的结点 $u\in V$。因为在删除 u（连同其邻接边）后的树中有 k 个结点，$e-1=k-1$ 成立。于是，有 $e=(k+1)-1=v-1$。

(2)⊢(3)。如果图不连通，则有 $s\geqslant 2$ 个连通且无回路的分支 $T_i=<V_i,E_i>$，$1\leqslant i\leqslant s$。因为每个 T_i 都是树，有 $|E_i|=|V_i|-1$，故

$$e=\sum_{i=1}^{s}|E_i|=\sum_{i=1}^{s}|V_i|-s=v-s\neq v-1。$$

这与题设矛盾。

(3)⊢(4)。$v=2$ 时，$e=v-1=1$，再增加一条边必产生回路，结论成立。

假设 $v=k$ 时命题成立。当 $v=k+1$ 时，因为图连通，无度为 0 的结点，故至少存在一个度为 1 的结点 $u\in V$。否则，若对每个 $v\in V$，有 $\mathrm{d}(v)\geqslant 2$，由握手定理，有

$$e=(\sum \mathrm{d}(v))/2\geqslant v。$$

与 $e=v-1$ 矛盾。

设与 u 邻接的结点为 v，删除 u 后的树为 T'。若在图中新加一条边(a,b)有 3 种情况：

(a) 与边(u,v)构成平行边，显然存在回路；

(b) 一个结点与 u 重合，另一结点与 T' 中的某结点 w 重合，因 v 与 w 连通，形成回路；

(c) 与 T' 内的两结点重合。因为 T' 有 k 个结点，由归纳法假定，必形成回路。参见图 8-33。

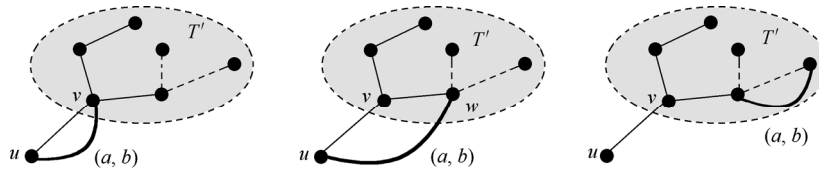


图 8-33

(4)⊢(5)。首先，T 必然是连通的，否则，在连通分支之间增加新边不会构成回路，与(4)的假设矛盾。其次，删除任一边一定不再连通，这是因为，若剩余部分仍连通，加上被删除的边就构成了回路，与无回路的题设矛盾。

(5)⊢(6)。因为连通，每对结点之间必然有路，但若某对结点之间有两条路就形成了回路，删去其中的一条边仍保持连通，与(5)的题设矛盾。

(6)⊢(1)。每对结点之间有路就是连通的定义。但如果存在回路，回路中的两结点之间就有两条以上的路，与(6)的题设矛盾。

[辨析] 这些定义是一些有关“什么是树？”的基本常识，练习在它们之间相互推证，可以帮助理解和掌握这些基本概念。

[辨析] 在 v 阶的图中，v–1 是保证图连通的最少边数。

[定理 8-20] 任何非平凡树 $T=<V,E>$ 中至少有两片树叶。

证明 若至多有一片叶子，记 $|V|=v$，则至少有 v–1 个结点的度均不小于 2。因此，由握手定理，有

$$e=\frac{\sum_{i=1}^{v}\mathrm{d}(v_i)}{2}\geqslant\frac{2(v-1)+1}{2}=v-0.5>v-1。$$

与 $e=v-1$ 矛盾。

例 8-10 若树 T 有 2 度、3 度和 4 度的分支点各 1 个，问该树有几片叶子？

解 设树 T 的叶子数为 x，则 T 的阶数（结点个数）为 x+3。由树的定义知 T 的边数为 $x+3-1=x+2$。由握手定理，得

$$2+3+4+x=2(x+2)。$$

解之得 $x=5$，即树 T 有 5 片叶子。

[辨析] 由于树的特殊性，分支点的状况在很大程度上决定了树的结构。

8.6.2 生成树

[定义 8-32] 若无向连通图 G 的生成子图 T 是树，则称 T 是 G 的**生成树**或**支撑树**（spanning tree）。T 中的边称为**树枝**，G 的不在 T 中的边称为**弦**。T 的所有弦与其关联结点的集合称为 T 的**余树**或**补**。

例如，图 8-34 中的 T 是 G 的生成树，T' 是 T 的余树。图 G 有 5 条树枝，4 条弦。

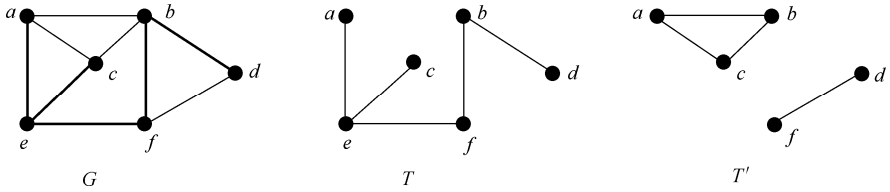


图 8-34

[定理 8-21] 任何连通图 G 至少有一棵生成树。

证明　若 G 无回路，则 G 本身就是树，也是其生成树。如果 G 中存在回路，则每次删除回路中的一条边，仍能保持图的连通性，直到不包含回路为止，得到树 T。因为 T 与 G 有相同的结点集，故是 G 的生成树。

[辨析] 一个图的生成树可能不是唯一的，它与边的删除次序有关。例如，图 8-35 也是图 8-34 中图 G 的生成树，但与 T 不同，也不同构。

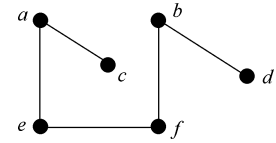


图 8-35

很明显，在一个具有 v 个结点，e 条边的图 G 中，其任何一棵生成树恰好有 v–1 条边（树枝），剩下的 e–(v–1) = e–v+1 条边就是弦。

因为树中不能有回路，故一个回路与树的余树之间一定存在着交集。

例 8-11　证明一条回路与任何一棵生成树的余树至少有一条公共边。

证明　因为生成树与其余树是互补的，合并后构成原来的图。如果一个回路 L 与某个树 T 的余树没有公共边，则说明 L 完全包含在树 T 中，但这是不可能的，因为树不能有回路。

[定理 8-22] 任何边割集与任何生成树至少有一条公共边。

证明　因为在图 G 中删除一个边割集后，G 不再连通，更不能得到任何连通子图，包括生成树。因此，要得到生成树至少要保留边割集中的一条边。

如果我们把图想象为一个通信网络，那么，生成树说明了要保证通信畅通，至少要保留哪些线路，以及怎样组成连接关系。通常，建立一条连接线路总是要付出一定代价的，如金钱和时间消耗等，故人们更关心能够达到最小费用的生成树，即带权图的最小生成树。

[定义 8-33] 一个**带权图**是指图的每个边被赋予一个描述代价的数（通常为非负值），称为权值，而图的权是指所有边的权之和。无向带权图也称为**网络**。

[定义 8-34] 在一个带权图 G 的所有生成树中，树权最小的生成树称为**最小生成树**（Minimum Spanning Tree，MST）。

以下是求最小生成树的 Kruskal（克鲁斯卡尔）算法。

[定理 8-23] 设图 $G=<V,E>$ 有 v 个结点，以下算法产生一个最小生成树 $T=<V,E_T>$：

(1) 令 $E_T=\varnothing$，选取权最小的边 e_1 加入 E_T，记边数 i=1；

(2) 若 $i=v$–1 结束，否则转(3)；

(3) 在 $E-E_T$ 中选择与 E_T 不构成回路且权最小的边 e_{i+1} 加入 E_T；

(4) $i=i$+1，转(2)。

此方法也称为“避圈法”，证明略。

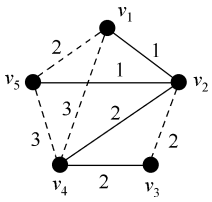


图 8-36

Kruskal 算法是一个简单的循环，可以先将所有边按权的大小升序排列，再从前到后逐个判别。若一个边与已加入树中的边不构成回路则加入树，否则舍弃。选够 v–1 条边结束。

例 8-12 求图 8-36 中的带权图 G 的最小生成树。

解 以下是构造最小生成树的过程：

(1) 先按权升序排列各边：

(v_1,v_2)，(v_2,v_5)，(v_1,v_5)，(v_2,v_4)，(v_2,v_3)，(v_3,v_4)，(v_1,v_4)，(v_4,v_5)。

(2) 逐个选择各边：

保留 (v_1,v_2)，保留 (v_2,v_5)，舍弃 (v_1,v_5)，保留 (v_2,v_4)，舍弃 (v_2,v_3)，保留 (v_3,v_4)，结束。

最后求得的最小生成树用实线边表示。

很明显，最小生成树不是唯一的，但树的权相同。

[延伸] Kruskal 算法是从边的角度计算最小生成树的，还有另一个比较著名的算法是 Prim 算法，该算法从点的角度计算最小生成树[49]。

[延伸] 除了最小生成树外，另一个与带权图密切相关的经典问题是最短路问题，即求出图中任意或指定两点 u 与 v 之间的最短距离。解决此问题的一个著名算法是由 Dijkstra 在 1959 年给出的，核心思想是将图的结点按邻接关系划分为不相交的子集 $S_0=\{u\},S_1,\cdots,S_{m-1},S_m=\{v\}$，再按下述方式对 $1\leqslant k\leqslant m$ 迭代计算

$$L_k(u,s)=\min\{L_{k-1}(u,s),L_{k-1}(u,x)+w(x,s)\}。$$

式中的 $L_k(u,s)$ 为结点 u 到 s 的最短路长度，$w(x,s)$ 为边 (x,s) 的权[7, 46]。

Dijkstra 算法可用于网络中的路由，以找到一条最经济的数据包投递线路。

8.6.3 根树

以下讨论有向图中的树。

1．根树及其相关概念

[定义 8-35] 一个有向图，如果略去各边的方向后所得到的无向图是树，则称其为**有向树**（directed tree）。如果一棵非平凡的有向树中恰有一个结点的入度为 0，其余结点入度均为 1，则称为**根树**（rooted tree）。

在根树中，入度为 0 的点称为**树根**（root）；入度为 1，出度为 0 的点称为**树叶**；入度为 1，出度大于 0 的点称为**内点**。内点和树根都是**分支点**。

例如，图 8-37 显示了一棵根树的原始画法和一般画法，其中，v_0 是树根，v_2 和 v_4 是内点，v_1，v_3，v_5，v_6，v_7 为树叶，v_0，v_2 和 v_4 都是分支点。

[辨析] 通常，在绘图时根树总是向下方或向右方生长，故边的方向可以略去不画。

[定义 8-36] 在根树中，从树根到任一结点 v 的路的长度称为 v 的**层数**，记作 $l(v)$，有时也直接称为**路径长度**。树 T 中结点的最大层数称为树的**深度**或**高度**，记作 $h(T)$。对任意结点 a 和 b，

若 $<a,b>\in T$，即 b 邻接到 a，称 b 是 a 的**儿子**，a 是 b 的**父亲**（或**双亲**）。若 a 和 b 的父亲相同，则称 a 和 b 是**兄弟**。若 $a\neq b$ 且 a 可达 b，称 a 是 b 的**祖先**，b 是 a 的**后代**（或**后裔**）。任何一个非根结点 a 及其后裔组成的子图是一棵以 a 为根的树，称为**根子树**。

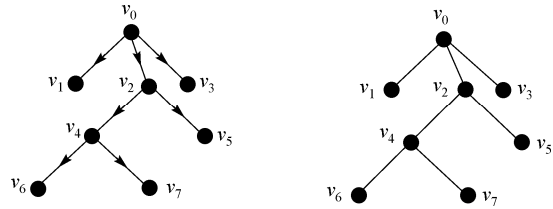


图 8-37

显然，根树可以看作是一个家族。在图 8-37 的树中，根 v_0 的层数为 0，为所有结点的祖先。树高 $h(T)=3$。v_2 是 v_4 和 v_5 的父亲，v_6 和 v_7 是 v_4 的儿子，二者是兄弟，v_0，v_2 和 v_4 都是它们的祖先。

[辨析] 这些概念是树中的一些常见名词，也是必须了解的常识。不过，应注意各类文献在一些定义上存在差异。例如，本书中定义根的层次为 0，但也可定义为 1；本书中认为树的深度与高度含义相同，但也可以仅定义其为树深，并令树高＝树深+1。

[定义 8-37] 在根树中，如果每一层上的结点都规定了次序，则称为**有序树**。

[定义 8-38] 设 T 是一棵非平凡根树。

(1) 若每个分支点至多有 r 个儿子，则称 T 为 ***r* 元树**或 ***r* 叉树**。$r=2$ 时的 r 元树就是著名的**二叉树**。

(2) 若 T 的每个分支点恰好都有 r 个儿子，则称 T 为 ***r* 元正则树**。

(3) 若 r 元正则树 T 的所有树叶的层数均为树高 $h(T)$，则称 T 为 ***r* 元完全正则树**或**满 *r* 叉树**。

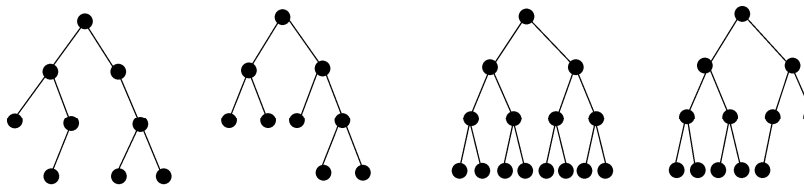
(4) 除最后一层外，每一层上的结点数均达到最大值，在最后一层上至多只缺少右边的若干结点的二叉树称为**完全二叉数**。或者说，完全二叉树是可以缺少最底层右边若干结点的满二叉树。

二叉树由于处理简单，在计算机领域的应用最为广泛，且任意一棵根树都可以转换为二叉树。

[辨析] r 元正则树也可以叙述为：每一个结点的出度都等于 r 或 0。在一些文献中，这种树就被称为完全 r 叉树，而本书中的完全 r 叉树指可能缺少最底层右边结点的满 r 叉树。

图 8-38 给出了以上定义的各种 r 叉树（$r=2$）的示例。

有时，如果 T 是一棵 r 叉树，也将 r 称为 T 的**阶数**，此时的阶数不表示树的结点数目。



(a) 二叉树　(b) 正则二叉树　(c) 满二叉树　(d) 完全二叉树

图 8-38

2．最优树

以下讨论二叉树中的典型问题，即求最优二叉树。

[定义 8-39] 若二叉树 T 有 t 片树叶 v_i，其层数为 $l(v_i)$，被赋予的一个权重为 w_i，$1 \leqslant i \leqslant t$，称 $\mathrm{WPL}(T)=\sum_{i=1}^{t} w_i \cdot l(v_i)$ 为 T 的权（Weighted Path Length of tree）。所有具有 t 片叶子且权值相同的树中，权最小的二叉树称为**最优二叉树**。

例如，图 8-39 中的 3 棵二叉树都带有相同的权 1、3、4、5、6，树的权分别是

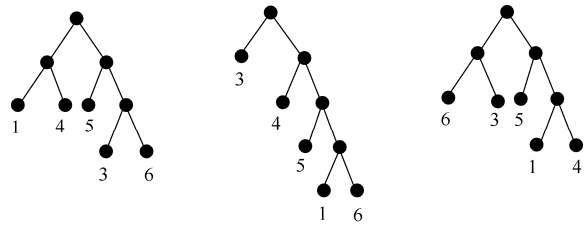
$$\mathrm{WPL}(T_1)=(1+4+5)\times 2+(3+6)\times 3=47,$$

$$\mathrm{WPL}(T_2)=3\times 1+4\times 2+5\times 3+(1+6)\times 4=54,$$

$$\mathrm{WPL}(T_3)=(6+3+5)\times 2+(1+4)\times 3=43。$$

实际上，它们都不是最优二叉树。

一种求最优二叉树的有效方法称为哈夫曼（Huffman）算法，图 8-40 给出了该算法的描述。



(a) T_1　　(b) T_2　　(c) T_3

图 8-39

Huffman 算法

输入：给定实数权值 $w_i, 1 \leqslant i \leqslant t$。

输出：最优二叉树。

(1) 用每个实数 w_i 单独作为结点并组成一棵子树 T_i，记 $S=\{T_i \mid 1 \leqslant i \leqslant t\}$；

(2) 选择两棵根的权最小的子树 T_i 和 T_j 作为儿子构造一棵二叉树，其根的权为 T_i 和 T_j 的根的权之和。将新的树加入 S，同时删除 T_i 和 T_j；

(3) 如果|S|=1 则输出并结束，否则，转(2)。

图 8-40

例 8-13　求带权 1、3、4、5、6 的最优二叉树及其权。

解　图 8-41 给出了根据哈夫曼算法计算最优二叉树 T 的过程，其中的(d)为最优二叉树，权 $\mathrm{WPL}(T)=42$。

3．最优前缀码

利用 Huffman 算法构造的最优二叉树可以用来产生最优前缀码。

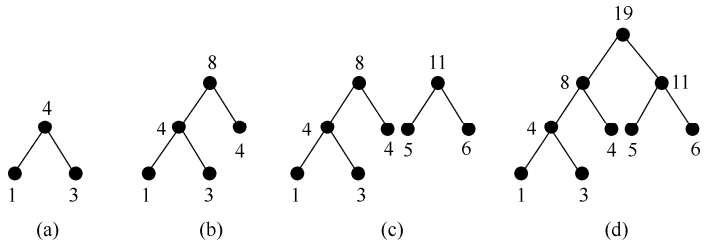


图 8-41

在计算机通信中，所有字符均需要用 0 和 1 组成的二进制串表示，称为编码。例如，字符 *A*、*B*、*C*、*D* 可分别用等长的串 00、01、10、11 表示。不过，在不同字符出现的频率不同时，采用不等长编码更为经济，但为了能够由一组编码串再切分出正确的字符编码，需要采用前缀码的编码方式。

[定义 8-40] 对于一个 n 位符号串 $\alpha=\alpha_1\alpha_2\cdots\alpha_n$，符号串 α_1、$\alpha_1\alpha_2$、…、$\alpha_1\alpha_2\cdots\alpha_{n-1}$ 称为 α 的长度为 1、2、…、n–1 的**前缀**。

若在一套编码方案（符号串集合）$\text{Code}=\{\beta_1,\beta_2,\cdots,\beta_m\}$ 中，任意两个符号串 β_i 和 β_j 互相不为前缀，则称 Code 为**前缀码**。而只用 0、1 构成符号串时就是 2 元前缀码。

[辨析] *互相不为前缀的码才称为前缀码。*

例如，$C_1=\{1,01,001,000\}$ 和 $C_2=\{00,10,11,011,0100,0101\}$ 是前缀码，而 $C_3=\{1,01,111,110\}$ 不是前缀码。

[辨析] *为什么不能互为前缀呢？至少是为了正确地切分出字符的编码。例如，当有一串二进制码 1110111 传来时，用 C_1 可唯一切分为 1、1、1、01、1、1，但用 C_3 会产生多种可能的切分，如 1、110、111 和 111、01、1、1，我们不知道怎样切分才是正确的。*

[定理 8-24] 对于任何一棵二叉树 *T*，只要将每个分支点的左儿子所在边标记 0，右儿子所在边标记 1（仅有一个儿子时 0、1 均可），则由根到所有叶子的路径上的边的标记组成的符号串集合构成前缀码。如果 *T* 是二叉正则树，则可产生唯一的一个 2 元前缀码。

证明　略。

例如，对于图 8-42 中的二叉树，依据标记产生了前缀码{00,10,11,010,0110,0111}。

如果知道了要传输符号的频率，可以利用这些频率作为权，用哈夫曼算法求出最优二叉树，再生成对应的前缀码。这样的前缀码可以使传输的二进制位最省，故称为“最佳前缀码”。

例 8-14　已知一次通信中采用 0～7 共 8 个字符，对应出现的频率为 30%、20%、15%、10%、10%、5%、5%、5%，求传输这些字符的最佳前缀码。

解　利用频率的整数部分作为权，依据哈夫曼算法求得最优二叉树，再依据定理 8-24 进行编码，得到 0～7 各字符对应的最优前缀码编码串为 01、11、001、100、101、0001、00000、00001。参见图 8-43。

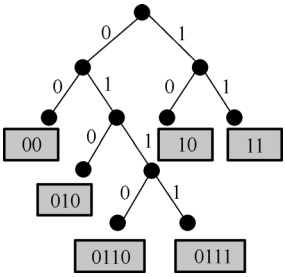


图 8-42

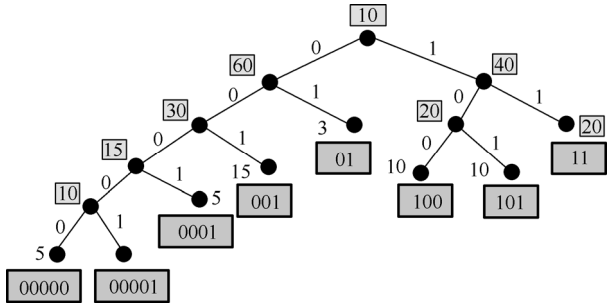


图 8-43

思考与练习 8.6

8-34 观察图 8-37 中的根树，找出下述结点或值：

(a) 根结点。 (b) 分支结点。

(c) 叶结点。 (d) 内点。

(e) 各结点的层。 (f) 各结点的父结点。

(g) 各结点的子结点。 (h) 树高。

(i) 所有子树。

8-35 证明满二叉树的结点个数必为奇数。

8-36 证明满二叉树的边的总数为 $2(n-1)$，其中的 n 为树叶数。

8-37 证明 n 阶满二叉树的树叶数目为$(n+1)/2$。

8-38 证明 n 阶完全二叉树的树高为$\lfloor \log_2 n \rfloor$，其中的$\lfloor x \rfloor$表示不超过 x 的最大整数。

8-39 求高为 h 的 r 元完全正则树的树叶数和分支点数。

8-40 利用 Kruskal 算法求图 8-44 的最小生成树。

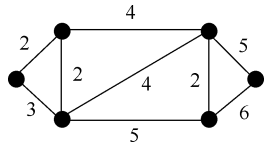


图 8-44

8-41 给定权 1、4、9、16、25、36、49、61、81、100，构造一棵最优二叉树。

8-42 说明下述符号串集合中哪些是前缀码。

(a) {0,10,110,1111}。 (b) {1,01,001,000}。

(c) {1,11,101,001,0011}。 (d) {b,c,aa,ac,aba,abb,abc}。

(e) {b,c,a,aa,ac,abc,abb,aba}。

8-43 设 7 个字符在一次通信中出现的频率为 a：35%、b：20%、c：15%、d：10%、e：10%、f：5%、g：5%，求传输这些字符的最佳前缀码。

附录 符 号 索 引

符号	含义	符号	含义
1（或 **T**）	真	$A \subseteq B$	集合 A 包含于 B
0（或 **F**）	假	$A = B$	集合 A 等于 B
$\neg$	否定	$A \subset B$	集合 A 是 B 的真子集
$\wedge$	合取，取下确界	$\|A\|$	集合 A 的元素个数或基数
$\vee$	析取，取上确界	U（或 E）	全集
$\bar{\vee}$	不可兼析取	$\varnothing$	空集
$\rightarrow$	条件	$\mathscr{P}(A)$或 2^A	集合 A 的幂集
$\leftrightarrow$	双条件	**R**	实数集
$\overset{c}{\rightarrow}$	条件否定	**Z**（或 **I**）	整数集
$\uparrow$	与非	**N**	自然数集
$\downarrow$	或非	**Q**	有理数集
$\Leftrightarrow$	逻辑等价	**C**	复数集
$\Rightarrow$	蕴含	$A \cap B$	集合 A 与 B 的交
P	前提引入规则	$A \cup B$	集合 A 与 B 的并
T	等价与蕴含规则	$A - B$	集合 A 与 B 的差
CP	CP 规则	$A \oplus B$	集合 A 与 B 的对称差
A^*	命题公式 A 的对偶式	$\sim A$ 或 $\overline{A}$	集合 A 的余集
$H_1, H_2, \cdots, H_n \Rightarrow C$	有效推理形式	$< x_1, x_2, \cdots, x_n >$	n 元组
$P \vdash Q$	由 P 推证 Q	$A_1 \times A_2 \times \cdots \times A_n$	笛卡儿积
$\forall$	全称量词	R	关系
$\exists$	存在量词	xRy	x 与 y 有关系 R
US（或 $\forall -$）	全称指定（消去）规则	$A \times B$	集合 A 到 B 的全关系，笛卡儿积
UG（或 $\forall +$）	全称推广（产生）规则	I_A	集合 A 上的恒等关系（函数）
ES（或 $\exists -$）	存在指定（消去）规则	M_R	关系矩阵
EG（或 $\exists +$）	存在推广（产生）规则	G_R	关系图
$x \in A$	x 属于集合 A	$x +_k y$	$(x + y) (\mathrm{mod}\ k)$
$x \notin A$	x 不属于集合 A	$x \times_k y$	$(x \cdot y) (\mathrm{mod}\ k)$
R^{-1}（或 R^C）	关系 R 的逆	$x \oplus_k y$	$[(x + y) (\mathrm{mod}\ k)]$
$R \circ S$	关系 R 与 S 的复合	$x \oplus_k y$	$[(x \cdot y) (\mathrm{mod}\ k)]$
$r(R)$	关系 R 的自反闭包	$A \cong B$	代数系统同构
$s(R)$	关系 R 的对称闭包	$\sigma\tau$	置换 τ 与 σ 复合
$t(R)$	关系 R 的传递闭包	S_n	n 元对称群
R^+	$\bigcup_{k=1}^{\infty} R^k$	aH	H 的左陪集
R^m	关系 R 的 m 次幂	Ha	H 的右陪集

续表

符号	含义	符号	含义
$C_R(A)$	R 生成的最大相容类	$<A,\preccurlyeq>$	偏序集，格
$[a]_R$	a 生成的 R 等价类	$\bar{a}$	a 的补元
A/R	商集	'	取补运算
$x \preccurlyeq y$	$<x,y>\in$ 偏序关系$\preccurlyeq$	$<B,\vee,\wedge,',0,1>$	布尔代数
$x \prec y$	$x \preccurlyeq y$ 且 $x \neq y$	$G=<V,E>$	图
COV(A)	盖住集	$<u,v>$	有向边
$m\|n$	m 整除 n	(u,v)	无向边
$x(\mathrm{mod}\ k)$	x 除以 k 的余数	$\mathrm{d}(v)$	结点 v 的度
$x \equiv y(\mathrm{mod}\ m)$	模 m 同余关系	$\mathrm{d}^+(v)$	结点 v 的出度
LUB	上确界	$\mathrm{d}^-(v)$	结点 v 的入度
GLB	下确界	$\Delta(G)$	最大度
GCD	最大公约数	$\Delta^+(G)$ 、 $\Delta^-(G)$	最大出度、最小出度
LCM	最小公倍数	$\delta(G)$	最小度
$\mathrm{dom}\,f$	前域，定义域	$\delta^+(G)$ 、 $\delta^-(G)$	最大入度、最小入度
$\mathrm{ran}\,f$	值域	K_n	n 阶无向完全图
$f:X\to Y$	函数，映射	$\bar{G}$	G 的补图
Y^X	集合 X 到 Y 的所有函数集合	$G_1 \simeq G_2$	图同构
$f(X)$（或 R_f）	f 的像集	$W(G)$	G 的连通分支数
f^{-1}	函数 f 的逆，即反函数	$d(u,v)$	结点 u 和 v 之间的距离
$g\circ f$	函数 f 与 g 的复合	$\kappa(G)$	G 的（点）连通度
card A（或$\|A\|$、$K[A]$、$\overline{\overline{A}}$）	集合 A 的基数	$\lambda(G)$	G 的边连通度
$\|A\|=\|B\|$（或 $A\sim B$）	集合 A 与 B 等势	$K_{m,n}$	完全二部图
$\aleph_0$	自然数集 **N** 的基数	$\deg(r)$	面 r 的次数
$\aleph$（或 C）	实数集 **R** 的基数	G^*	G 的对偶图
Z_m	$\{[0],[1],\cdots,[m-1]\}$	$\chi(G)$	G 的着色数
N_m	$\{0,1,\cdots,m-1\}$		

参 考 文 献

[1] 牛连强，冯海文，侯春光. C 语言程序设计——面向工程的理论与应用[M]. 北京：电子工业出版社，2013.

[2] Rosen K. H.著，袁崇义，屈婉玲，张桂芸译. 离散数学及其应用（第 6 版）[M]. 北京：机械工业出版社，2011.

[3] 左孝凌，李为鑑，刘永才. 离散数学[M]. 上海：上海科学技术文献出版社，1982.

[4] 邓辉文. 离散数学[M]. 北京：清华大学出版社，2006.

[5] 张清华，蒲兴成，尹邦勇，等. 离散数学[M]. 北京：机械工业出版社，2010.

[6] 石纯一，王家. 数理逻辑与集合论[M]. 北京：清华大学出版社，2000.

[7] Garnier R，Taylor J. Discrete Mathematicsfor New Technology (2nd Ed.)[M]. London: Institute of Physics Publishing，2002.

[8] 陈光喜，丁宣浩，古天龙. 离散数学[M]. 北京：电子工业出版社，2008.

[9] 屈婉玲，耿素云，张立昂. 离散数学（第 2 版）[M]. 北京：清华大学出版社，2008.

[10] 王树禾. 离散数学引论[M]. 北京：中国科技大学出版社，2001.

[11] 乔维声. 离散数学（第 3 版）[M]. 西安：西安电子科技大学出版社，2004.

[12] 杨洪圣，张英杰，陈义明. 离散数学[M]. 北京：科学出版社，2011.

[13] 徐小萍. 命题逻辑演绎推理在日常生活中的应用[J]. 襄樊学院学报，2007，28(11): 13-16.

[14] 王文龙. 命题逻辑在判断推理中的应用[J]. 计算机教育, 2014, (24):89-93.

[15] 牛连强，陈欣，邓金鹏. 小议离散数学课程中的应用示例与教学[J]. 高等理科教育，2008, (3): 35-38.

[16] 张微. 数理逻辑中谓词逻辑推理错误的分析[J]. 合肥学院学报, 2012, 22(4): 1-7.

[17] 赵卯生. 对谓词逻辑在人工智能科学中应用的分析[J]. 山西高等学校社会科学学报, 2001, 13(2): 67-69.

[18] 王万良. 人工智能及其应用[M]. 北京：高等教育出版社，2008.

[19] 让人惊讶的十个悖论.http://jandan.net/2013/12/18/10-paradoxes.html，2015.

[20] 崔屹. 图像处理与分析——数学形态学方法及应用[M]. 科学出版社, 2002.

[21] 黄海龙, 王宏, 李微. 一种基于数学形态学的签名真伪鉴别方法[J]. 东北大学学报(自然科学版), 2011, 32(6): 854-858.

[22] 李杰, 彭月英，元昌安，等. 基于数学形态学细化算法的图像边缘细化[J]. 计算机应用，2012，32(2):514－516，520.

[23] 王珊，陈红. 数据库系统原理[M]. 北京：清华大学出版社，2003.

[24] 牛月，吴美云，罗嘉悦，等. 等价关系及其应用[J]. 高师理科学刊，2015, 35(2): 22-25.

[25] 吴国兵. “离散数学”中的等价关系[J]. 计算机教育，2009, (1): 50-52.

[26] 王燕. 基于等价关系的关联规则挖掘算法研究[J]. 计算机工程与应用，2006，42(8): 187-189.

[27] 李克润，周贤善. 等价关系在计算机科学中的应用研究[J]. 长江大学学报(自科版)，2004, 1(2/3): 33-35.
[28] 丁树良，罗芬. 由偏序关系的可达阵导出 Hasse 图的有效算法——兼谈其在认知诊断中的作用[J]. 江西师范大学学报（自然科学版），2013, 37(5): 441-444.
[29] 邹又姣，冉占军，王晓峰. 偏序关系哈斯图的一种求解方法[J]. 高等数学研究，2013, 16(1): 55-57.
[30] 李信巧，周生明. 集合的基数与元素个数[J]. 广西师范大学学报(自然科学版)，2000, 18(1): 28-31.
[31] 千溪. 谈谈集合的基数[J]. 数学通报，1979, (2): 22-28.
[32] 伽罗瓦群论的诞生. http://www.wxphp.com/wxd_97lal1eabj9epjx24kor_1.html, 2015.
[33] 邓明立.置换群概念的历史演变[J]. 自然辩证法研究，1995, 11(1): 14-19, 28.
[34] 包芳勋，付夕联，张玉峰，等. 群的概念及思想方法[J]. 曲阜师范大学学报，1994, 20(4): 101-106.
[35] 曹建秋，黄英. 用置换群解决信息加密问题的探索[J]. 重庆交通学院学报, 2001, 20(S): 131-132.
[36] Richard A.Brualdi著，冯速译. 组合数学[M]. 机械工业出版社，2012.
[37] 陈欣，牛连强，李兆明. 由划分、等价关系到陪集与 Lagrange 定理——离散数学中几个相关概念教学方法刍议[J]. 高等理科教育，2014, (6): 50-54.
[38] 李尚志. 抽象代数的人间烟火[C]. 大学数学课程报告论坛论文集：2009，北京：高等教育出版社，2010.
[39] 冯克勤. 有限域及其应用[M]. 大连：大连理工大学出版社，2011.
[40] 李超，杜绍平，梁昊. 有限域的算术软件及其编码密码应用[J]. 计算机应用与软件，2000, (5): 36-40.
[41] 祁永谨. 布尔代数及其应用简介[J]. 数学教学研究，1982, (1): 37-48.
[42] 祁永谨. 布尔代数及其应用简介（续）[J]. 数学教学研究，1982, (2): 42-51.
[43] 宋晓奎，李秀平. 二部图的匹配的简单应用[J]. 邢台学院学报，2012, 27(4): 169-170.
[44] 许小满，孙雨耕，杨山，等. 超图理论及其应用[J]. 电子学报，1994, 22(8): 65-71.
[45] 夏菁，刘真，胡越琦，等. 基于超图的骨生物数据可视化[J]. 计算机辅助设计与图形学学报，2011, 23(12): 2041-2024.
[46] 卢鹏丽，贾春旭，沈万里. 基于二部图的公共交通网络模型[J]. 计算机工程，2012, 38(3): 265-266, 269.
[47] 王耀宣，叶俊民，陈静汝，等. 一种基于二分图故障检测模型的软件故障定位方法研究[J]. 计算机科学, 2013, 40(6): 160-163.
[48] 卜月华. 图论及其应用[M]. 南京：东南大学出版社，2002.
[49] MarkAllenWeiss著，冯舜玺译. 数据结构与算法分析：C 语言描述（原书第 2 版）[M]. 北京: 机械工业出版社，2004.